NOTE

This Microfiche meets the quality requirements of the American National Standard for Microfiche of Documents (ANSI PH5.9-1975). However, because of imperfections in the document from which it was made, it contains images that are illegible or difficult to read. The source document for this microfiche is the best copy that could be obtained prior to filming.

CIS Congressional Information Service, Inc.
Washington, D.C.

TECHNICAL PROPOSAL
US 84-10/12
SURVEILLANCE: HISTORICAL POLICY REVIEW
SUBMITTED BY HERMAN SCHWARTZ

March 15, 1985

This contractor document was prepared by an outside contractor as an input to an ongoing OTA assessment. It does not necessarily reflect the analytical findings of OTA, the Advisory Panel, or the Technology Assessment Board.

J952-51

March 15, 1985

TECHNICAL PROPOSAL
US 84-10/12
SURVEILLANCE: HISTORICAL POLICY REVIEW
SUBMITTED BY HERMAN SCHWARTZ

EXECUTIVE SUMMARY

The clash between privacy and security, between civil liberties on the one hand and law enforcement, national security, or effective administration on the other, has been overstated. Nevertheless, there is a tension between them.

The history of electronic surveillance is an illuminating illustration of our society's failures and successes in resolving this tension. The lesson from this story seems equally applicable to the new technologies, and it is this: The courts, on their own, and relying solely on elemental constitutional principles and concepts, rarely have either the will or the capacity to respond effectively to the new technologies. The courts--which, in this context, means the Supreme Court--continually tries to pour the new wine of technology and technique into the old conceptual bottles but it doesn't do it successfully.

Equally unavailing are administrative and regulatory approaches: The administrative rules are often disregarded; the agency head will frequently choose to ignore violations that come to his attention if they result from excessive zeal; administrative rules themselves are easily changed.

Only the legislative, often after judicial fumbling and failure, can adopt the measures that go even some way toward reconciling the conflicting and varying needs. Even with

legislation, political forces may impede an optional solution, and judicial interpretations may frustrate legislative intent.

Historical Review

When electronic surveillance abuses developed in the the early 1920s, the Justice Department voluntarily adopted a ban on wiretapping. The Treasury Department's Bureau of Prohibition continued to tap, however, and in 1930, Justice resumed wiretapping though purportedly only for serious offenses.

In 1927, the Supreme Court in a 5-4 decision refused to bring wiretapping under the Fourth or Fifth Amendment, because it did not involve a trespass. Olmstead v. U.S., 277 U.S. 438 (1928). Congress failed to pass any significant corrective legislation until 1934 when it adopted §605 of the Communications Act. There is no legislative history to indicate that even then Congress intended to deal with wiretapping in this legislation. Nevertheless, section 605 was interpreted in 1937 by the Supreme Court to bar all wiretapping by federal offices and others. Nardone v. U.S., 302 U.S. 379 (1937). Congressional efforts to overturn this decision were unsuccessful. In the meantime, however, the Justice Department construed §605 in such a way as to allow it to tap, and in 1940 President Franklin D. Roosevelt authorized limited wiretapping for national security purposes.

In 1942, the judicial pendulum swung again and the Court reaffirmed Olmstead in a microphone surveillance case. The FBI and other federal agencies engaged in very extensive wiretapping and bugging during the 1940-1965 period as the Roosevelt authorization was extended to domestic matters (1946) and the FBI was given unrestricted authority to bug rooms (1954).

Between 1959 and 1968, interest in electronic surveillance increased as widespread illegal surveillance by public and private individuals was disclosed and concern about organized crime increased. In 1967, the Supreme Court overruled Olmstead in Katz v. U.S., 389 U.S. 347, and in 1968, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act, allowing federal and state officials to use electric surveillance to intercept conversations if authorized by a court pursuant to an elaborate set of procedures. 18 U.S.C. §2500ff.

Experience under this statute with law enforcement surveillance indicates widespread surveillance of many people and conversations at a very substantial cost in privacy and money; the harm to the fabric of trust, the creation of an atmosphere of fear, and the impact on constitutional rights of expression and association, are almost impossible to quantify, but may be very significant.

The court-order system of supervision seems to work poorly at the state level and in a flawed fashion at the federal level; many of the statutory safeguards do not seem to be working as intended.

The statute seems to have had little effect on illegal surveillance, but that is very difficult to assess because there is inevitably little data on so secret a practice.

There is controversy over the law enforcement benefits from the statute because it is difficult to establish criteria for evaluating these benefits, and to obtain the necessary data. Some believe that except for some highly publicized cases, the benefits do not seem very great; others believe it is of great value.

Policy options are available to deal with these and other problems, though political realities may preclude most of these. The options include:

1. Abolishing all law enforcement surveillance. This is both politically unrealistic and would be totally unacceptable to federal and many state law enforcement officials.

2. Repealing state authority. This is also politically impossible, as is a less drastic measure that would reduce the list of crimes for which state officials may use electronic surveillance.

3. Limiting surveillance authority to a few serious crimes.

4. Eliminating or reducing the authority to use microphone surveillances, while extending it to include certain crimes not now covered, *e.g.*, witness trampering.

5. Last-resort use--tightening up the requirements.

6. Minimization--requiring both a good faith effort and objective minimization in light of the particular situation.

7. Emergency use--expansion to include life-threatening situtations.

8. Suppression sanction for proven violations--Congressional specification of when suppression is appropriate.

9. Periodic reports--making them mandatory and in all federal--and state--cases.

National security intelligence has been the subject of elctronic surveillance since 1940. It was subject only to supervision by the Attorney General insofar as wiretapping was concerned, and only to internal FBI controls with respect to "bugs". The 1976 Report of the Senate Select Committee on Intelligence documented many abuses by the FBI, the CIA and other intelligence agencies. In 1972, the Supreme Court prohibited electronic surveillance for domestic security purposes, U.S. v. U.S. District Court, 407 U.S. 297 (1972) and in 1978 Congress enacted the Foreign Intelligence Surveillance Act, 50 U.S.C. §1800ff., authorizing a secret court order procedure for foreign intelligence gathering by means of electrical or other mechanical devices.

Intelligence surveillance has an inherently broader sweep than law enforcement surveillance, and oversight and control are more problematic because of the secrecy involved , as well as the difficulty involved in evaluating the relative costs and benefits of this practice. There has been a significant increase in the number of FISA surveillance since 1979, but there is no way for an outside observer to evaluate the significance of this. There is cause for concern about the effectiveness of judicial oversight, especially since judges are particularly deferential where foreign intelligence and other foreign policy matters are concerned.

One party surveillance is virtually unregulated by the federal statute; some states have restricted it. There are federal administrative regulations, but these seem to have little effect in controlling the practice. Recent efforts to enact legislative controls have been unsuccessful. Possible policy options include:

1. Prohibiting official taping that is not for law-enforcement or intelligence-gathering purposes.
2. Administrative controls similar to those under the Privacy Protection Act of 1980.

3. Prohibiting one-party consent to remove multi-party conversations from Title III where only one or a few of the persons being overheard are suspected of criminality.

New technologies have been considered by the Supreme Court in certain recent cases, and the Court has failed to respond to the dangers inherent on them. Rather, it has adopted traditional conceptual frameworks and distinctions, which have generally resulted in denying protection to the latter; it has frequently invoked waiver and assumption-of-risk concepts to deny protection to records in the possession of third parties, and to one-party consent transmissions, respectively it has tended to minimize the significance of certain new technologies by referring to them as only "sense-enhancement." The rather general criterion for constitutional protection--whether the Court believes "society is prepared to recognize an expectation of privacy as reasonable," Katz v. U.S., 389 U.S. at 361 (Harlan, J., concurring)--has enabled the Court to evade many hard issues of reconciling privacy and the legitimate needs of law enforcement by simply declaring, in a conclusory manner, that something is not a "reasonable" expectation.

Legislative options to respond more adequately to the threats to privacy posed by these new technologies ought to be considered. These options include:

1. Title III--inclusion of beepers, pen registers and videotaping under Title III and the Foreign Intelligence Surveillance Act (where beepers and pen registers are concerned).

2. Beepers--requiring judicial authority for use of beepers for surveillance of activities outside the house, under a lesser standard.

3. Pen registers--requiring either Title III or conventional Fourth Amendment safeguards.

4. Videotaping--requiring safeguards going beyond Title III because of the greater threat to privacy, and barring it entirely where many if not most people videotaped are not suspects.

Illegal surveillance by private parties has probably not been significantly reduced. Illegal surveillance by foreign governments is a matter shrouded in such secrecy because of national security considerations, that it is almost impossible for an outsider to evaluate.

TECHNICAL PROPOSAL
US 84-10/12
SURVEILLANCE: HISTORICAL POLICY REVIEW
SUBMITTED BY HERMAN SCHWARTZ

March 15, 1985

TABLE OF CONTENTS

Introduction 1

I. Historical Review--1920-84.................................. 3
  1920-27--The Period Prior to Olmstead v. United States.................................. 3
  1927-33--From Olmstead to §605.......................... 5
  1934-41--Section 605 and the Pre-war Period........... 11
  A Note on Congressional Ineffectuality................. 15
  1942--Electronic Surveillance during World War II................................ 16
  1946-1960--The Post-war period prior to The Kennedy Administration...................... 18
  1960-68--Events leading to enactment of Title III.. 22

II. Current Issues 34
  A. Title III 34
    1. Experience under the Act......................... 34
      a. The cost of electronic surveillance...... 38
      b. The benefits................................ 39
      c. The court-order protections............... 47
      d. General implications...................... 54
    2. Policy options.................................. 54
  B. National Security Intelligence Surveillance........ 61
    1. The legislative history of FISA.............. 62
    2. Problems arising out of intelligence surveillance.............................. 63
  C. One-Party Consent Surveillance.................... 70
    Policy options.................................. 72

III. New Technologies...................................... 74
  A. Judicial Decisions.................................. 74
    Policy options.................................. 85

IV. Illegal Electronic Surveillance By Private parties and foreign governments............ 88
  A. Private Parties..................................... 88
  B. Foreign Government Surveillance.................... 91

Appendix: Chronology of Key Events and Decisions
  Congressional Action 1914-59
  Federal Use of Electronic Surveillance in Narcotics Cases
  Federal Use of Foreign Intelligence Surveillance Act Surveillances

Bibliography

March 15, 1985

TECHNICAL PROPOSAL

US 84-10/12

SURVEILLANCE: HISTORICAL/POLICY REVIEW

SUBMITTED BY HERMAN SCHWARTZ

INTRODUCTION

A historical/policy review of how we have dealt with surveillance issues in the last 65 years gives cause for uneasiness as to how we will cope with the burst of new surveillance technology that has confronted us since World War II. Miniaturization, increased penetration, and reduced expense have all come together to reduce exponentially the natural physical protections for personal privacy. If privacy is indeed, as Justice Louis D. Brandeis put it many years ago, "the right most valued by civilized men, the right to be let alone," and if it is indeed the indispensable condition for exercising rights of free expression and free association guaranteed by our Constitution, our society will have to do a better job at protecting privacy that it has until now.

The problem involves both will and ingenuity. There must be a high valuation of this right and imaginative ways to protect it, without unduly interfering with security and other basic social goals. To some extent, the clash between privacy and security, between civil liberties on the one hand and law enforcement, national security, or effective administration on the other, has been overstated. Nevertheless, there is a tension between them that often results in some impairment of one against the other.

The history of electronic surveillance is an illuminating illustration of our society's failures and successes in this regard. The lesson from this story is one that seems equally applicable to the new technologies, and it is this: the courts, on their own, and relying solely on constitutional principles and concepts, have neither the will nor the capacity to respond imaginatively and effectively to the new technologies. Only the legislature, often after judicial fumbling and failure, can adopt the measures that go some way toward reconciling the conflicting and varying needs, qualify with legislative and judicial influence on that. The courts--which, in this context, means the Supreme Court--continually tries to pour the new wine of technology and technique into the old conceptual bottles but it doesn't do it successfully, and it becomes the job of the legislature to clean up the mess. Partly, this is because the Supreme Court has generally been law enforcement oriented, except occasionally, such as the 1961-67 period. Partly also, this is because new ways of thinking about these problems are necessary and courts are not very adept at that.

Equally unavailing are administrative and regulatory approaches. The administrative rules are often simply disregarded, and the agency head will frequently choose to ignore violations if they result from excessive zeal. Administrative rules are also subject to easy change.

A legislative solution is not, of course, a panacea. It often creates many new problems, and judicial interpretations can sometimes frustrate legislative intent. But only legislation offers the opportunity for a combination of fine-tuning and meaningful sanctions, that judicial and administrative approaches do not.

I. HISTORICAL REVIEW--1920-84

1920-27--The period prior to Olmstead v. United States.

Telegraph and telephone tapping by both private citizens and public officials began soon after these devices were invented. Some state laws tried to deal with telephone tapping either through their trespass statutes or by expanding early laws barring telegraph interceptions; the legality of official surveillance under these statutes was usually unclear, though the absence of a rule excluding illegally obtained evidence in most jurisdictions made that immaterial. Nevertheless, by 1927, some 28 states had made wiretapping a crime. See *amicus* brief for the telephone companies in *Olmstead v. U.S.* 277 U.S. 438 (1928).

Federal concern first surfaced in 1918 when the federal government took over the telephone system, but the concern was only for "the protection of the government and the property of the telephone and telegraph companies while under governmental control." H. R. Rep. No. 800, 65th Cong., 2d Sess. (1918), reprinted in Wiretapping, Eavesdropping and the Bill of Rights, Hearings Before the Subcommittee on Constitutional Rights of the Senate Judiciary Committee, Part 4, Appendix to Part 3, 86th Cong., 1st Sess. 792 (1959) ("1914-1959 Leg. Hist."). The statute barred tapping of or interference with telephone and telegraph messages, if the tap was done "without authority." The legislation expired in 1919.

Civil liberties and related concerns first became important in the early 1920's, when wiretapping became a notorious weapon of the Department of Justice in the so-called Palmer Raids against aliens. Westin, The Wire-tapping Problem, 52 Colum. L. Rev. 164, 172 n.35 (1952). There were also many reports that the phones and offices of members of Congress had been eavesdropped upon.

In the wake of the Teapot Dome and other scandals, Harlan Fiske Stone was made Attorney General in 1924. He promptly banned wiretapping by Department of Justice personnel, including the Bureau of Investigation (the FBI's predecessor). The Bureau's 1928 Manual listed wiretapping first among "Unethical Tactics." Warrantless FBI Electronic Surveillance, Supplementary Detailed Staff Reports, Book III, Final Report of the Senate Select Committee to Study Government Operations With Respect to Intelligence Activities, 94th Cong., 2d Sess. 277 (1976) ("III Church Comm.").

This effort at administrative control was only partially successful at best, for reasons that may be endemic. For one thing, the order bound only the Justice Department and not the

Treasury, which had jurisdiction over Prohibition enforcement, the law enforcement area that came to rely most on electronic surveillance. Prohibition agents, therefore, continued to wiretap, even though the Treasury purported to be officially opposed to wiretapping. Murphy, Wiretapping on Trial 13 (1965). Such partial coverage of an administrative directive may be frequent, especially if--as appeared in hearings during the 1950s--military and national security agencies also engage in the practice and are exempt from the order, either expressly or otherwise.

1927-1933--From Olmstead to § 605.

The Treasury's wiretapping ultimately brought the matter to the courts which it is now universally acknowledged, failed adequately to respond. The major case was, of course, Olmstead v. United States, 277 U.S.438 (1928).

Olmstead was the biggest bootlegger in Western Washington, Murphy 16, and the Court was led by Chief Justice William Howard Taft, who put a very high value on law enforcement, and especially on enforcement of the Volstead Act; in 1926 he had told a Collier's magazine writer that the public should not be overly scrupulous about police methods against criminals. Id. at 83.

The Court split 5-4, and in an opinion by Chief Justice Taft ruled that neither the Fourth nor Fifth Amendments to the Constitution applied to wiretapping; by implication from the fact that Justice Brandeis' dissent raised First Amendment considerations which the Court did not even discuss, the First Amendment was implicitly held not to apply either.

Olmstead's Fifth and First Amendments rulings are still applicable. Electronically obtained evidence is still not considered a form of self-incrimination, Hoffa v. United States, 385 U.S. 293 (1966), and the First Amendment was deemed only relevant, and was not the basis for the decision in U.S. v. U.S. District Court, 407 U.S. 297 (1972), despite the stated link between freedom of expression and invasions of personal security noted both in that case and as far back as the eighteenth century in England in the Wilkes Cases (1763-1770).

The Fourth Amendment was the primary constitutional provision that was arguably applicable and Chief Justice Taft's refusal to bring electronic surveillance under that amendment determined the treatment of electronic surveillance for 40 years, until Olmstead was overruled in Katz v. United States, 389 U.S. 347 (1967).

The Court gave three reasons why the Fourth Amendment was not implicated: officials had not trespassed onto Olmstead's property; the Amendment did not apply to intangibles like speech but only to material "effects"; and there was no protection for voice communication projected outside the house.

Justice Holmes wrote a short dissent, condemning the agents' conduct as "dirty business." Justice Brandeis wrote the main dissent in which he disagreed with the majority's reading of the precedents, its very narrow view of the Fourth Amendment, and its willingness to countenance criminal activity by the government.

For him, the Fourth Amendment was designed to protect individual privacy, and he warned that the "progress of science in furnishing the Government with means of espionage" called for a flexible reading of the amendment to "protect the right of personal security." He stressed that because a tap reaches all who use the phone, including all those who either call the target or are called, "writs of assistance or general warrants are but puny instruments of tyranny and oppression when compared with wiretapping." The telephone companies' amicus brief had also argued against a narrow view of "seizure" or a limitation to "tangibles," as had the dissent below. 1914-59 Leg. Hist 770-73.

The public reaction to the Olmstead decision was largely and strongly negative. Murphy 125. It settled the law, however, and the matter was not up to Congress and/or the Executive Branch. Immediately after Olmstead was decided, bills were proposed to ban wiretapping. 1914-59 Leg. Hist. 881-83. In January, 1931 two and a half years after Olmstead, Congressman Tinkham of Massachusetts offered an amendment to the Justice Department Appropriations Act, providing "that no part of this appropriation shall be used for the tapping of telephone or telegraph wires." 74 Cong. Rec. 2901 (Jan. 22, 1931). Relying heavily on the Brandeis and Holmes dissents and on J. Edgar Hoover's testimony before the Appropriations Committee that the practice was "unethical" and grounds for immediate dismissal, and pointing to the inconsistency between Bureau of Investigation and Bureau of Prohibation practices, he attacked wiretapping as "contemptible and despicable." Id. at 2902.

The issue was clearly caught up in the struggle between "wets" and "drys" over Prohibition. Thus "wet" Congressman Beck of Pennsylvania, a supporter of the Tinkham amendment, noted the "moral fanaticism that is behind the enforcement of the eighteenth amendment," (2902), whereas "dry" Congressman Finley from Kentucky asked whether the "wets" would find "any kind of evidence . . . acceptable to them for [any] prosecution . . .[under] the prohibition law." (2905) The "drys" had a solid majority in the House, despite "wet" gains in 1930, see N.Y. Times, Nov. 5, 1930, p.1, and defeated the amendment, 78-99. Id. at 2906.

Two years later, Prohibition was on its way out, and this time the wiretap opponents succeeded, the only time Congress deliberately went on record against electronic surveillance. The wiretap issue was tied up with other alleged abuses in enforcement of the Prohibition laws involving entrapment and the purchase of evidence, and no one seriously challeged the wiretap ban. Indeed, most of the oratory favoring the amendment was aimed against entrapment. See 76 Cong. Rec. 4235-4242 (Feb. 16, 1933). The ban was largely an empty victory, however, for it applied only to wiretapping for Prohibition enforcement. Enacted in February 1933, 47 Stat. 1381, it was effective only until December 5, 1933, when Prohibition ended. The wiretap ban was obviously tied to the growing disenchantment with Prohibition, or at least with its enforcement--"wets" had won a solid majority in both Houses in the 1932 election, N.Y. Times, Nov. 9, 1932, p.1, and the 21st Amendment repeating Prohibition was sent to the

States on February 20, 1933, just a few days after the wiretap ban was passed by the Senate.

The major change during this period was administrative. Despite the Treasury policy against wiretapping noted above, the Bureau of Prohibition continued to wiretap but Treasury officials did nothing to stop it. In 1930, Congress transferred the Prohibition Bureau to Justice, producing a conflict between the wiretap policies of the Bureau of Prohibition and the Bureau of Investigation. This conflict was resolved by a change in the 1924 Stone order to allow both Bureaus to wiretap; the policy was justified by Attorney General William Mitchell as necessary for kidnap cases. Murphy 131-32. The Mitchell policy limited wiretapping to very serious cases, and required authorization by the Assistant Attorney General. III Church Comm. 278. It appeared, however, that the FBI used wiretapping in Mann Act prosecutions as well. See Lowenthal, The Federal Bureau of Investigation 19 (1950).

The Court's treatment of wiretapping, and the subsequent administrative and legislative actions, illustrate some of the difficulties in accommodating new technologies. The judicial response insisted on a narrow traditional conceptualism that refused to consider changing conditions. This response was not, however, dictated by legal logic or precedent, nor was it a function of the unavailability of alternatives: no precedents limited the Fourth Amendment to a trespass or to tangibles and a clear precedent--the application of the Fourth Amendment to the mails in Ex parte Jackson, 96 U.S. 727 (1878)--justified application of the Amendment to the projection of communications outside the house. The Court majority was fully aware of this, since the telephone companies and four Justices had urged a broader construction to accommodate changing technology. All to no avail.

Obviously, explanations beyond the opinion are only conjectural. But it is hard to ignore the strong concern for law enforcement over individual liberty reflected in a letter from Chief Justice Taft to his brother a week after the decision:

> "The telephone might just as well have been used to carry on a conspiracy to rob, to murder, to commit treason. The truth is we have to face the problems presented by new inventions. Many of them are most useful to criminals in their war against society and are at once availed of, and these idealist gentlemen urge a conclusion which facilitates crime by their use and furnishes immunity from conviction. . . ." Murphy 125.

As previously noted, this has been the attitude of most Supreme Court Justices during the last 50 years; it is especially prevalent today in drug cases, for as Justice John Paul Stevens and others have observed, the Court seems particularly eager to eliminate obstacles to effective drug law enforcement. Florida v. Rodriguez, 105 S.Ct. 308, 311 (1984) (dissent); see also LaFave, I Search and Seizure § 2.7, 1984 Pocket Part p. 112 (1984).

At the very least, this early history illustrates how little one can rely on the courts to respond in the first instance to the threats to civil liberties posed by new technologies. Insofar as balancing liberty against law enforcement is seen as the problem, the Court will usually choose law enforcement, even though nothing in precedent, logic or other conventional legal sources, precludes a different balance.

As noted, administrative regulation offers little more comfort. The Justice Department regulation applied only to Justice personnel, thus omitting the government officials who did the most surveillance. And when a policy conflict developed--which may be simply another way of saying that when it appeared that the regulation would apply to the only area where it really counted--the regulation was abandoned by a stroke of a law enforcement official's pen. Even the remaining restrictions limiting the technique to serious crimes was sufficiently vague to justify its evasion by other prosecutors.

Finally, the period also saw some congressional activity, as some legislators tried to legislatively overturn the Olmstead decision. Except for the rather insignificant 1933 legislation, the effect of which was short-lived, those efforts were unsuccessful. This sputtering reaction was a sign for the future: civil libertarians were unable to overcome the concern about tying the hands of the police.

1934-41--Section 605 and the pre-war period.

In 1934, Congress recodified the Radio Act of 1927, itself a recodification of legislation going back to 1912. Section 605 of the 1934 Act provided that "No person not being authorized by the sender shall intercept any communication and divulge . . . the contents . . . " There was no specific legislative history for this section and it appears that the 1934 bill was not intended to change existing law. See S. Rep. No. 781, 73d. Cong., 2d Sess. 11 (1934), reprinted in 1914-59 Leg. History 895; Report of the National Commission for the Review of Federal and State Laws relating to Wiretapping and Electronic Surveillance 35 (1976) ("NWC Report"; hearings and staff studies of the Commission will be cited as "NWC Hgs." and "NWC Staff Studies"). Apparently no one thought Congress had taken an important step in dealing with electronic surveillance.

In thus came as a surprize to many, if not most, when the Supreme Court in 1938 ruled that §605 prohibited all telephone wiretapping, even when done by federal government officers, Nardone v. U.S., 302 U.S. 379 (1937). In 1957, the Court ruled that this applied to state officers as well. Benanti v. U.S., 355 U.S. 96 (1957). The Nardone decision was generally criticized both in 1938 and later as "judicial legislation". See NWC 35.

Congressional response to Nardone was swift, but again ineffectual. This time, bills were introduced to allow wiretapping, provided that the head of a department believed a felony had been or was about to be committed by two or more people--the bill was expressly limited to felonies. Concern about organized crime was the main consideration:

> As a result of this decision, the Federal law-enforcement officers are forbidden to listen in on communications by wire and radio, with the result that the organized underworld is at full liberty to make restricted use of the wire and radio facilities of the Nation to carry on their rackets and schemes to the detriment of the public. Organized gangsterdom finds itself today in possession of a most powerful weapon with the assurance of immunity for its use even in cases involving murder where the only evidence available is that secured by interception.
>
> In addition to murderers and others there are counterfeiters and gangs operating nationally and internationally in the smuggling and disposition of narcotic

> drugs and other contraband, as well as gangs engaged in kidnaping, violating the internal-revenue laws, and racketeers of high and low degree who are now at liberty to plan and carry out their schemes through the use of wire- and radio-communication facilities of the Nation without fear of detection by the interception of their communications, or punishment based on evidence secured by that means. In this connection it should not be overlooked that the prohibition against interception of communications applies to officers of the Secret Service of the United States, an agency of the Treasury Department, charged with responsibility for the safety of the President. Such officers are forbidden today under the interpretation of section 605 in the Nardone decision, to intercept any communications of suspected persons.

See S. Rep. No. 1790, 75th Cong., 3d Sess. 3 (1938), reprinted in 1914-59 Leg. Hist. 958-59. Interestingly enough, the Attorney General did not provide wholehearted support for the bill, saying only:

> It is manifest that indiscriminate use of wire-tapping should not be practised by law-enforcement officers. On the other hand, a complete proscription of such evidence and of such methods of investigation may at times result in a failure to detect or apprehend a person guilty of a grave offense. Whether a criminal or suspected criminal should be completely protected in his right of privacy or whether, in the interests of society, an invasion of such right of privacy should be permitted under the restrictions and limitations proposed in the pending measure, involves a question of balance which is peculiarly within the province of the legislative branch of the Government.

Id. at 690.

Congressional concern about organized crime remained one of the two primary reasons for authorizing electronic surveillance (the other was national security). Bills passed both houses, but the session ended before the conference committee could resolve a slight difference between the two bills--the House bill explicitly criminalized unauthorized official surveillance. Id. at 961; Murphy 135.

The ease with which both Houses passed bills allowing federal surveillance might lead one to think legislation was imminent. That was not to happen, even though despite the Nardone decision, the Federal government (and state officials, see generally Dash, R.F. Schwartz and Knowlton, The Eavesdroppers (1959) ("Dash")), continued to wiretap. In fact, legislation was not introduced in the 1939 session of Congress, and by 1940, other approaches took over, particularly as concern shifted to national security issues. Moreover, concern about the dangers of wiretapping continued. See S. Rep. No. 1304, 76th Cong., 3d Sess. (1940).

Part of the reason for the absence of legislation is that is was probably unnecessary for those who wanted to continue to use electronic surveillance. Upon taking office as Attorney General, Robert H. Jackson at first banned all wiretapping, Order No. 3343 (Mar. 15, 1940), while asserting that wiretapping should be legislatively authorized in a "limited class of cases such as kidnapping, extortion and racketeering". The House of Representatives thereupon passed a Joint Resolution, seeking to authorize wiretapping, though in national security matters only, declaring:

> The committee would hesitate to allow wires or short wave messages to be tapped in times of normalcy. We are, however, in a national emergency. Some sacrifices must be made. Some rights may have to be yielded. Just as in a period of war, the writ of habeas corpus may be abrogated and certain inalienable rights temporarily suspended, so in times of danger and peril--although short of war--inroads must necessarily be made upon those rights, if out Democracy is to be preserved.

Jackson approved this proposal. H.R. Rep. No. 2574, 76th Cong., 32 Sess. 2(1940), reprinted in 1914-59 Leg. Hist. 965-68. The matter became moot, however, when President Franklin D. Roosevelt authorized Jackson to approve wiretaps on "persons suspected of subversive activities against the United States." III Church Comm. 278-80. Moreover, at some point after Nardone the Department construed §605 as not prohibiting wiretapping itself, but only the interception and subsequent divulgence outside the federal establishment. Ibid. This construction was criticized by many as tortuous, but it remained in effect until 1968 and was the basis for the Department's continuing use of wiretapping, discussed below.

A Note on Congressional Ineffectuality 1929-41

Congressional action during these early years seems quite ineffectual and almost irrelevant, even though there was a lot of it. Thus:

--The initial effort by opponents of wiretapping and/or Prohibition to ban use of the technique in the immediate aftermath of Olmstead failed, because of opposition from both the Justice Department and the Bureau of Prohibition.

--These opponents were ultimately successful two years later in 1933, when Congress forbade the Bureau of Prohibition--but not any other federal agency--from using any appropriations money to wiretap. But Prohibition ended that year and the legislation had little impact. Moreover, it is not clear whether this legislation was primarily aimed at wiretapping or at Prohibition.

--Congress passed a statute, §605 of the Communications Act, but apparently had no intention to affect wiretapping with it. The Court interpreted §605 in the *Nardone* case to reach electronic surveillance but the quick negative reaction of Congress--bills overturning *Nardone* easily passed *both* houses--indicates Congress was not happy with the Court's reading. This Congressional action was ineffectual, however, for although both Houses acted in a similar fashion and passed similar bills, they allowed rather slight differences between the two bills to prevent the passage of legislation. --Even this latter non-action by Congress had little effect, for just as another branch of government--the Supreme Court--had acted in place of Congress when the Court decided *Nardone*, so now the Executive Branch acted in place of Congress' failure to overrule *Nardone* by (1) the Justice Department's construing §605 in a way to render it of little significance, and (2) the President's issuing an Executive Order to allow national security surveillance regardless of *Nardone* and §605.

In short, Congress clearly sputtered during this period and succeeded in accomplishing little that it tried to do, despite the enactment of two pieces of legislation in 1933 and 1934 and the passage in 1938 of similar bills in House and Senate.

1942-45--Electronic surveillance during World War II.

Throughout the prior period, attention had been focused on telephone tapping, with an interplay among courts, the legislature and the executive branch. During the late 1930's, the Court had been the primary protector for privacy with Nardone and its progeny. After World War II began, the judicial pendulum swung again.

Surveillance of rooms came before the courts for the first time in Goldman v. United States, 316 U.S. 129 (1942). The Court adhered to Olmstead and ruled that since the microphone surveillance in that case did not involve a trespass--the bug was placed against the outside of a wall--it was not protected by the Fourth Amendment; the Court also ruled that § 605 did not apply. The Court devoted virtually no time to any of the defendants' arguments, simply citing Olmstead and refusing to overrule it. Justice Frank Murphy, as had Justice Brandeis before him, laid out the consequences of ignoring the many technological advances in investigatory technique, and the need for the Constitution to keep pace with these advances, id. at 139-40, but to no avail.

The special issues raised by microphone surveillance (as compared with telephone tapping), were hardly noticed in the opinions and yet they are significant. Justice Murphy noted that microphone surveillances reach into the home or office, areas that are usually considered private, so that at least one of the Olmstead rationales--the Constitution provides no protection for voices projected outside--had no applicability. Not noted, however, was that it is difficult to limit such surveillances to the suspects, since many people come into a room. As a result, highly confidential and even legally privileged conversations may be overheard, even though they may be quite irrelevant to the subject matter of the investigation, and the central protection provided by the Fourth Amendment--limiting the search to particular items as to which there is probable cause to believe they are involved in criminality--is difficult to provide.

1946-1960--The post-war period prior to the Kennedy Administration.

During 1946-59 the executive branch continued to play the primary role. Congress passed no legislation though bills were introduced and informative hearings were held; the courts did relatively little that fundamentally affected electronic surveillance law or practice, except for two decisions decided the same day. In the first, telephone conversation that are intercepted with the consent of one party to the conversation were excluded from § 605 protection, Rathbun v. U.S., 355 U.S. 107 (1957); in the second, it was made clear that § 605 did indeed apply to state officials like those in New York who had been openly tapping and bugging. Benanti v. U.S. 255 U.S. 96 (1957). The Rathbun decision was in the spirit of an earlier decision during this period, On Lee v. United States, 343 U.S. 747 (1952) that refused to grant any Fourth Amendment protection against informers, even if they were secretly and simultaneously transmitting their conversations with the suspect to the police. This refusal to protect against betrayals of confidence, even when facilitated by new technology, has also been reaffirmed in recent years. U.S. v. White, 401 U.S. 745 (1971); the conceptual framework--that we all assume the risk of betrayal by someone we trust--has also been retained.

The central events of this period were administrative. The first was Attorney General Tom Clark's successful effort in 1946 to get President Truman to authorize the Justice Department to engage in warrantless wiretapping for "cases affecting the domestic security or where human life is in jeopardy" on the basis of President Roosevelt's prior directive of 1941 relating to international security matters; Clark apparently did not transmit to Truman that portion of the Roosevelt letter which ordered that the investigations be limited "insofar as possible to aliens." When Truman was later apprised of these changes from the Roosevelt order, he had an order drafted paralleling Roosevelt's, "but for reasons that are unclear, it was never issued." III Church Comm. 282-83.

The other major administrative act was by Attorney General Herbert H. Brownell in 1954. In 1952, Attorney General J. Howard McGrath prohibited warrantless microphone surveillance in all cases involving a physical intrusion into the premises under investigation. In 1954, the Supreme Court made it clear that a warrantless microphone surveillance involving a trespass violated the Fourth Amendment, Irvine v. California, 347 U.S. 128 (1954), though it refused to apply the exclusionary rule under the then-applicable law. Nevertheless, when the FBI protested the McGrath policy to Attorney General Brownell, he reversed his predecessor's position. On May 22, 1954, Brownell authorized "unrestricted use of this technique in the national interest." (emphasis added), with Attorney General approval not required. III Church Comm. 295-97. Thus, even though as Attorney General

Nicholas deB. Katzenbach noted later, "'bugs' . . . are far more serious invasions of privacy than are taps, ['bugs'] were not subject to the authorization [by the Attorney General] procedure until . . . March 30, 1965." III Church Comm. 298 n.85a.

The primary congressional activity was an attempt in the early 1950s to enact legislation allowing wiretapping in national security cases--as was tried in 1940--which was unsuccessful.

Throughout the 1948-59 period, numerous bills, authorizing electronic surveillance were introduced. See 1914-59 Leg. Hist. 785-89. None was enacted into law though occasionally one passed in the House. Congress was aware of the many problems raised by this inaction--House Judiciary Committee Chairman Emanuel Celler noted many of them in his opening statement in the 1955 House Hearings. See Hearings before Subcommittee No. 5, House Jud. Comm., 84th Cong., 1st Sess. 1-2 (1955). The hearings disclosed both alleged needs and claimed abuses, but the legislative impasse continued.

During the war and post-war years, the FBI engaged in massive amounts of electronic surveillance. The FBI has conceded that between 1940 and 1960, it installed over 7,000 national security surveillances, with 519 taps and 186 bugs in 1945 alone, the high point. The Treasury was also busy. On his retirement, the Treasury's chief wiretapper admitted to having installed over 10,000 taps during 1934-48. Other federal agencies, like the military, also did a lot of tapping and bugging. On the local level, the New York City police installed thousands of taps each year (3,588 in 1953-54, for example), mostly in morals and bookmaking investigations; studies by Samuel Dash and others documented widespread police tapping elsewhere. See Dash *passim*. Almost all tried to hide the fact that they were tapping. See Schwartz *Taps* 9.

The tapping and bugging targeted many people who would not normally seem to be appropriate targets, a situation that continued into the 1960s at least. In 1941, for example, the Los Angeles Chamber of Commerce was tapped, on the authority of Attorney General Francis Biddle. Presidential aides and others were similarly tapped. The most complete information on these practices, as developed by the Church Committee, relates to FBI surveillances in the post-1960 period when Dr. Martin Luther King Jr., Congressman Harold Cooley, journalists and many others were put under electronic surveillance; there is no reason to think that the practice was any different in the 1942-60 period. See generally III Church Comm. 315-32. There is also no reason to think that widespread surveillance by other government agencies--the CIA, the military, the Treasury--was any more discriminating. See Wiretapping Hearings before Subcomm. No. 5. House of Representatives Judiciary Committee, 84 Cong., 1st Sess. 53, 67 (1955). ("1955 Hearings").

Several other events were crucial during this period, raising issues of continuing concern. The publication of *The Eavesdroppers* by Dash, R.F. Schwartz & Knowlton in 1959 documented in detail what was widely suspected: wiretapping by state officials was widespread, uncontrolled, and abused, even where a court order system was in effect. See also 1955

Hearings 170, 180, 191-92, 215-17, 223, 292-302; but see id. at 314-33 (Hogan testimony). Questions were also raised as to the effectiveness of electronic surveillance and of judicial protections, as well as the persistent use of electronic surveillance in state law enforcement for minor crimes. Id. at 194, 347, 359. There was also much documentation of illegal private wiretapping, by private detectives and others for industrial espionage and in domestic relations matters, and of the ineffectiveness of either federal or state law to cope with this.

The other significant event during this period was the greatly increased concern about organized crime, fueled in part by a meeting of suspected organized crime leaders in Appalachia, New York, and by congressional hearings conducted by the McClellan Committee in which Robert F. Kennedy participated.

1960-68--Events leading to enactment of Title III.

During this period, electronic surveillance became a major public issue, with forces pushing in competing directions. All branches of the federal government--legislative, executive, and judicial--played a major role in bringing matters to a head with the 1968 legislation which authorized electronic surveillance for law enforcement purposes; a similar process was to occur in the 1969-78 decade with respect to electronic surveillance for national security purposes.

The tension in this issue between liberty and order was heightened by two events mentioned earlier. On the one hand, the Apalachin meeting in 1957 finally induced FBI Director J. Edgar

Hoover to turn FBI efforts against organized crime, which he had earlier resisted, and to resort to widespread and lengthy use of electronic surveillance for that purpose.

On the other hand, the Dash, R.F. Schwartz & Knowlton book, together with hearings in 1958 and 1959 by Senator Thomas Hennings (D.-Mo.), Chairman of the Senate Constitutional Rights Subcommittee, highlighted the dangers of uncontrolled wiretapping.

In 1961, Robert F. Kennedy became Attorney General and he made the attack on organized crime a major priority. He authorized wiretapping and FBI Director Hoover, acting under the 1954 Brownell order, engaged in a great deal of microphone surveillance, apparently on his own. The Treasury Department joined in the campaign against organized crime and also engaged extensively in electronic surveillance.

To resolve some of the legal problems, the Kennedy Administration introduced legislation to allow court-ordered wiretapping for law enforcement purposes; the Department refrained from asking for authority for microphone surveillance, and refused to endorse such legislation proposed by others because of the difficult constitutional issues involved. Navasky, Kennedy Justice 78 n.8 (1971). Consistent with the position of his predecessors, the Attorney General refused to accede to a requirement that national security surveillances also be judicially authorized; it was generally believed that this refusal blocked passage of this legislation; the Senate hearings on the bill also revealed a continuing hostility to all kinds of wiretapping on the part of many Senators.

Competing pressures continued throughout the 60s. The President's Commission On Law Enforcement and Administration of Justice issued a report in 1967, and near the top of its priorities was organized crime. While it did not explicitly recommend the legitimation of wiretapping, a majority of the Commission did so. The American Bar Association proposed a statute which became the model for the legislation permitting wiretapping that was ultimately enacted in 1968.

Because of this intensive activity, the arguments for this technique was spelled out quite clearly. Thus, Professor G. Robert Blakey, the chief draftsman of both the ABA report and proposals and of the 1968 Wiretap Act, told a Congressional committee in 1967:

> The normal criminal situation deals with an incident, a murder, a rape, or a robbery, probably committed by one person. The criminal investigation normally moves from the known crime toward the unknown criminal. This is a sharp contrast to the type of procedures you must use in the investigation of organized crime. Here in many situations you have known criminals but unknown crimes.
>
> So it is necessary to subject the known criminals to surveillance that is, to monitor their activities. It is necessary to identify their criminal and noncriminal associates; and their areas of operation, both legal and illegal. Strategic intelligence attempts to paint this broad, overall picture of the criminal's activities in order that an investigator can ultimately move in with a specific criminal investigation and prosecution.

Hearings on Controlling Crime Through More Effective Law Enforcement before the Subcommittee on Criminal Laws and Procedures of the Senate Judiciary Committee, 90th Cong., 2d Sess. 957-58 (1967). (emphasis added).

The pressures were not all one-sided, however. In the mid-1960s, illegal tapping and bugging by the FBI, IRS, and others came to light when FBI bugs were accidentally discovered in a Las Vegas gambler's office and in Washington's Sheraton-Carlton Hotel and, as in so many other instances, lawyer-client conversations were overheard. This led to a series of court-ordered revelations of illegal federal surveillance, involving some 50 or more cases. As a result, in 1965 President Lyndon B. Johnson ordered an end to all electronic surveillance except in national security cases. III Church Comm. 298-300.

At the same time, hearings chaired by Senator Edward V. Long (D.-Mo.) discovered that despite a 1938 Treasury directive banning electronic surveillance, IRS agents had tapped and bugged extensively, set up some 24 bugged conference rooms, and engaged in breaking and entering. Other agencies were also discovered to have tapped and bugged widely. One Federal Bureau of Narcotics agent testified that he had broken into homes "hundreds of times" in the 1950s to install microphone surveillances. If caught, he reported, his instructions were to deny that he had been authorized to do by his superiors. Electronic surveillance by the Food and Drug Administration, the Post Office, and other federal agencies was also revealed. See generally _Invasions of Privacy_, Hearings before the Subcommittee on Administration Practice and Procedure of the Senate Judiciary Committee, 89th Cong. (1965-66).

During this period, the Supreme Court finally overruled _Olmstead_, in _Katz v. U.S._ 389 U.S. 347 (1967), after first striking down the New York wiretap statute in _Berger v. New York_, 388 U.S. 41 (1967). Prior to being specifically overruled, Olmstead had been gradually eroded, first by the Court's extension of Fourth Amendment protection to (intangible) conversations in Irvine v. California, supra and then by a gradual whittling away of the trespass requirement. See Silverman v. U.S., 365 U.S. 505 (1961) and Clinton v. Virginia, 377 U.S. 158 (1964).

The Katz decision set out both a general formula for the interests protected by the Fourth Amendment and specific criteria for a statute authorizing law enforcement wiretapping--it expressly excluded national security surveillance from its discussion. See 389 U.S. at n.21.

The general formula has come to focus on whether an expectation of privacy is "one that society is prepared to recognize as 'reasonable.'" 389 U.S. at 361 (Harlan, J., concurring). This is the basic test that the Supreme Court has applied to all investigative techniques that raise privacy problems; the problems with this test will be discussed below, when it is applied to the various new technologies.

The Court's specific criteria for a valid surveillance involved the conventional magistrate's warrant, and the equally conventional particularization and probable cause requirements applied to a specific telephone, for a specific need and crime, to the specific suspect's conversations and the specific time during which he spoke. The Court also stressed that prior notice to the suspect of the interception was unnecessary, and indicated that notice after the interception was constitutionally acceptable. These requirements were drawn from prior related cases and from conventional Fourth Amendment principles.

All these factors, plus a growing concern about crime, finally came together with the explosive events of 1968 to break the 30-year impasse since Nardone and produced Title III of the Omnibus Crime Control and Safe Streets Act of 1986, 18 U.S.C. §2500ff, which authorizes electronic surveillance. Although it is usually difficult to point to one factor as decisive, particularly after 40 crowded years, it does seem that the key factor was the assassination of Robert F. Kennedy. Many of those including the writer, who were close to events, are convinced that it was that single event which overwhelmed opposition in the House, where it was thought the legislation would continue being bottled up. See Harris, Annals of Legislation--The Turning Point, The New Yorker, (Dec. 14, 1968). pp. 68-179. Indeed, Harris commented that:

> all those who voted against it, and most of those who didn't vote at all [believed] the bill was a piece of demagoguery, devised out of malevolence and enacted in hysteria.

Id. at 68.

Title III authorizes telephone tapping and microphone surveillance by federal and state officials, if antecedent judicial approval was obtained. Because it may serve as a model for other types, detailed analysis of the statute may be useful.

The basic legislative history document, S. Rep. No. 1097, 90th Cong., 3d Sess. (1968), sets out the purpose of the statute as follows:

> [T]he U.S. Supreme Court, on June 12, 1967, handed down the decision in Berger v. New York, 388 U.S. 41, which declared unconstitutional the New York State statute authorizing

> electronic eavesdroppoing (bugging) by law-enforcement officers in investigation certain types of crimes. The Court held that the New York statute, on its face, failed to meet certain constitutional standards. In the course of the opinion, the Court delineated the consitutional criteria that electronic surveillance legislation should contain. Title III was drafted to meet these standards and to conform with Katz v. United States, 389 U.S. 347 (1967).
>
> Title III has as its dual purpose (1) protecting the privacy of wire and oral communications, and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized. Id. at 66.

The "Problem" the statute was designed to solve, was seen as a combination of "tremendous scientific and technological developments that have taken place in the last century [that] have made possible today the widespread use and abuse of electronic surveillance techniques," and "a body of law [that] from the point of view of privacy or justice [i.e., law enforcement] is . . . totally unsatisfactory". Id. at 67,69.

The preamble to Title III reflects these aims: (1) to obtain evidence of "certain major types of offenses," and to cope with "organized criminals"; and (2) to safeguard the privacy of innocent persons and to provide "assurances that the interception is justified and that the information obtained thereby will not be misused." The legislative history specifies that the major purpose of Title III is to a combat organized crime." S. Rep. No. 1097, 90th Cong., 2d Sess. 70 (1968), although Senator John L. McClellan (D-Ark.) the principal sponsor of Title III made clear his concern about other matters when he noted that he also wanted to allow eavesdropping on black militants. 114 Cong. Res. S 6197, S61199 (daily ed. May 23, (1968); see §2516(1)(a).

In order to achieve these purposes, the statute provides that electronic surveillance of conversations is prohibited, upon pain of a substantial jail sentence and fine, except for: (1) law enforcement surveillance under a court order; (2) certain telephone company monitoring to ensure adequate service or to protect company property; (3) surveillance of a conversation where one participant consents to the surveillance; and (4) surveillance covered by the Foreign Intelligence Surveillance Act of 1978. Law enforcement surveillance must meet certain procedural requirements, which include:

(1) an application by a high-ranking prosecutor (not by a policeman);

(2) surveillance only for one of the crimes specified in Title III (the list was expanded in the early 1970s);

(3) probable cause to believe that a crime has occurred, that the target of the surveillance is involved, and the evidence of that crime will be obtained by the surveillance.

(4) a statement indicating that other investigative procedures are ineffective;

(5) an effort to minimize the interception.

A judge must pass on the application and may issue the order (and any extensions) if it meets the statutory requirements. Shortly after the surveillance ends, notice of the surveillance must be given to some or all of the people affected, as the judge decides, unless the judge agrees to postpone the notice. Illegally obtained evidence may not be used in any official proceedings, and a suit for damages may be brought for illegal surveillance, though a very strong good faith defense is allowed. In addition, the manufacture, distribution, possession, and advertising of devices for electronic surveillance for non-public use are prohibited.

There was little discussion of electronic surveillance by _state_ officials during the legislative debates, since most of the discussion centered on organized crime, and with some exceptions, the states have played almost no role in fighting organized crime. Nevertheless, §2516(2) of Title III gives state officials wiretapping authority if a state passes legislation modeled on the federal act for the investigation of "murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marijuana or other dangerous drugs, or other crime dangerous to drugs, or other crime dangerous to life, limb or property and punishable by imprisonment for more than one year . . . or any conspiracy to commit any of the foregoing offenses." As of December 31, 1983, some 29 states and the District of Columbia have authorized their law enforcement officials to wiretap, though the state statutes differ in various ways.

On its face Title III covers the interception of audible conversations only; data transmission, the videopart of videotaping, pen registers, and other non-audible forms of communications are not covered; see S. Rep. No. 1097 at 90 (pen registers, etc., not included). The statute also permits interception for official purposes where one of the parties to the conversation has consented to the interception; private interceptions where one party consents, are also exempt from the statutory ban unless the interception is for a criminal, "injurous," or tortious purpose. Evidence obtained in violation of the statute is excluded from all judicial or administrative proceedings, but only someone whose privacy was invaded can challenge the evidence.

The statute is one of the first and probably the most elaborate effort of cope with the problems raised by the new technologies. The path to the legislation illustrates what may well be a recurrent pattern:

> The judicial system at first refuses to confront the threat to civil liberties posed by a new technology, even though the legal, analytical and factual resources are available for a more sensitive response.
>
> The threat seems so serious, however, that the executive branch tries to restrain itself, an effort that fails because of the strong and recurrent pressures to use the new technology. Efforts at a legislative response fail, because of political and other conflicts, even though hearings are held and problems are aired. The judiciary begins to try to impose some controls over the new technology, see Nardone, Silverman, Katz, but the efforts are inadequate and incomplete. The legislature finally steps in to tailor measures specifically designed to accommodate the conflicting interests.

That is the history of law enforcement wiretapping, and it was repeated with respect to intelligence surveillance and other matters; see below. Obviously, such a course is not inevitable. Olmstead was a narrow 5-4 decision that could easily have gone the other way with Brandeis writing the majority opinion; Goldman's application of Olmstead to microphone surveillance could have been decided differently, as could have Nardone's interpretation of §605; Olmstead could have been overruled in Goldman or in On Lee, two other very close decisions.

Nor need it have taken Congress so long to act. In other Fourth Amendment contexts, it has responded much more quickly to Supreme Court decisions it did not like, see e.g., Privacy Protection Act of 1980, 42 U.S.C. §2000a-11, responding to Zurcher v. Stanford Daily, 436 U.S. 547 (1978) (intrusions on newsrooms), although that situation did involve a response to a very powerful political force that felt itself damaged by the decision--the press.

Nevertheless, the pattern of events leading to the wiretap legislation is likely to be a typical one and it does point strongly to one conclusion: judicial or administrative protections are likely to be unavailable or inadequate. What is less clear is whether we must repeat the legislative failure to act effectively until long after the problems surface. Whatever the merits or demerits of Title III, it clearly represents a very tardy response to a problem that first became apparent 40 years earlier with Olmstead. The Foreign Intelligence Surveillance Act of 1978 represents a somewhat quicker response, though here too, problems related to national security surveillance were brought to congressional attention as early as 1940, see p. 14 above, some 38 years before the FISA Act, and were seen to be quite serious by the early 1950's.

II. CURRENT ISSUES

The current period has seen three important phenomena: (1) the operation of Title III with respect to law enforcement wiretapping and bugging; (2) the Foreign Intelligence Surveillance Act of 1978; and (3) the judicial, legislative and administrative responses to new technologies. Also touched on will be illegal surveillance by both private persons and foreign governments.

A. Title III.

1. Experience under the Act.

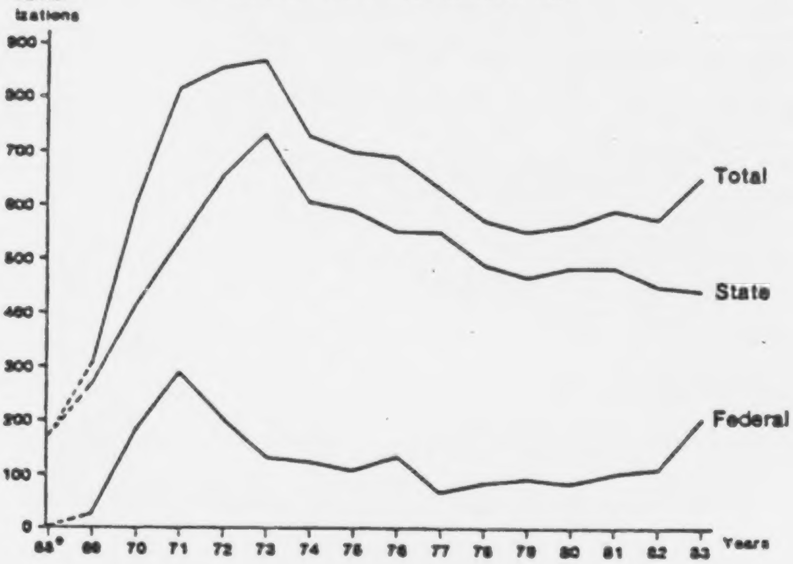
Since June 1968, when Title III became effective, federal officials have installed almost 2000* electronic surveillance. During that same period, state officials installed over 7400* with the bulk of the state usage occurring in three states: New York, New Jersey and Florida. As of December 31, 1983, 29 states and the District of Columbia had authorized law enforcement wiretapping, but many of these invoked this authority rarely and in a good number of states, not at all. See Report of Applications for Orders Authorizing or Approving The Interception of Wire or Oral Communications (Wiretap Report), issued by the Administrative Office of the U.S. Courts. 1968-83 ("19--Wiretap Report"). In 1983, for example, 11 of these states did no wiretapping at all. 1983 Wiretap Report 7.

---

*The figures are only approximate, for there are reporting lags in the Annual Reports of the Administrative Office of the U.S. Courts, from which these figures are taken.

The pattern of usage has varied very significantly. A chart prepared by the Administrative Office tells some of the story graphically:

Number of State and Federal Intercept Authorizations
Calendar Years 1968 through 1983



*Reporting period was from June through December 1968.

1983 Wiretap Report 2.

As the chart shows, State usage has steadily fallen since 1973, whereas federal usage rose to a peak in 1971, dropped sharply during 1973-80, and is now on a very sharp rise.

The usage by offense also varies markedly, particularly on the federal level. Whereas state usage has tended to concentrate on gambling and narcotics, federal usage initially concentrated on gambling but then changed. The emphasis on gambling disappeared by 1973, and overall tapping fell. Federal narcotics tapping during the first 10 years of the Act averaged about 30/year but there has recently been a change in policy, and narcotics wiretapping in 1982-83 averaged 114/year; the figure is expected to be much higher in 1984. Use of wiretapping in racketeering (RICO) prosecutions has also been high in recent years. Wiretapping is used only occasionally for murder, sabotage, kidnapping, robbery or other completed crimes.

Each installation, particularly at the federal level, catches scores of people and hundreds of conversations. In 1983 for example, the average reported federal tap caught 177 people in 2057 conversations, which reportedly comes to 36,816 people overheard in more than 427,000 conversations.

In 1983, the average federal interception cost $65,000, but this figure understates the cost by a very substantial amount because it omits the cost of the lawyers' and judges' time in preparing and passing on the application. See NWC Report 57; Goldsmith, The Supreme Court and Title III: Rewriting the Law of Electronic Surveillance 74 J. Crim. L. & Criminology 1, 160-62 (1983) (hereafter "Goldsmith").

From 1973 through 1981, 12741 convictions were reportedly obtained. Of the investigations that utilized wiretaps, drug cases produce the highest rate of convictions. In 1981-82, for example, 43% of drug-related installations were associated with convictions but only 25% of the other installations.

The Supreme Court has dealt with many aspects of the statute, and though that Court has never passed on its constitutionality, nine circuit courts have sustained it, e.g., U.S. v. Sklaroff, 506 F.2d 837, 840 (5th Cir. 1975), and the constitutional validity of Title III is not in doubt.

The Supreme Court and the lower courts have interpreted the statute in a way generally helpful to law enforcement. They have, for example, ruled that police are not required to make even a good faith effort to minimize their interceptions, Scott v. U.S., 436 U.S. (1978), and that a warrant may authorize intercepting the calls of unknown third parties, not just the targeted suspects. U.S. v. Kahn, 415 U.S. 143 (1974). Lower courts have made it clear that the so-called "last resort" requirement of the statute--a showing that other techniques are unavailable--is not to be stringently applied. NWC Report 66-67; NWC Hearing at 607-08, 618. See generally, Goldsmith, supra.

The experience under Title III raises numerous policy issues of very far-reaching significance for all forms of intrusive technologies. The include the following:

(1) On the assumption that electronic surveillance does indeed intrude on privacy and threaten civil liberties an assumption conceded by proponents as well as opponents, see Blakey and preamble to Title III), do the benefits in improved improve law enforcement exceed the losses and expenses?

(a) Can one quantify the costs, monetary and otherwise?

(b) Can one quantify the benefits? By what criterion are they to be measured? Are there structural or other inherent variations, e.g., by offense? How reliable are the data on which to make such an assessment?

(2) Are there differences in the cost-benefit balance between microphone surveillances and telephone tapping?

(3) Are the judicial and other protections effective? By what criteria?

(4) What are the implications of the above for other new technologies?

a. The cost of electronic surveillance.

It appears that many thousands of people are overheard in hundreds of thousands of conversations. A rough estimate for the last seven years of reported Title III electronic surveillance (1977-83) based on Administrative Office Reports is that 3900 taps and bugs were installed, and 370,000 people overheard. For 1983 alone, federal tapping reportedly listened in on 36,816 people in over 427,000 conversations.

The number of people and conversations overheard is rising, as the federal tapping shifts to narcotics law enforcement and racketeering where the surveillance is much longer, and much more is listened to, in the hope of gathering some clues. As a result, a vast number of these people and conversations that are overheard are quite innocent, and many of the conversations may be confidential or even legally privileged.

The monetary costs are also very high. As noted, the average federal tap reportedly cost $65,316 in 1983, and this is necessarily an understatement, for the reasons mentioned earlier. The total reported 1983 cost, just on the federal level was over $13,000,000, and probably much more than that; the total 1983 reported cost for both federal and state surveillance was approximately $20 million, 1983 Wiretap Report 14, again substantially understated.

What one cannot quantify or even estimate are the psychological costs, and the harm, if any, to freedom of speech and association. Although use of wiretapping for drug, gambling or racketeering enforcement would not seem to have political aspects, drug enforcement on the state level--and perhaps on the federal level as well--was linked to police action against dissident Black and other groups in the 1960s, and that may still be the case. Moreover, the sweep of the RICO statute (Racketeer Influenced and Corrupt Organizations) is so broad that many innocent people who fear that they are in some way involved with someone under suspicion of a RICO violation, such as business or family associates, may think themselves potential wiretapping or bugging targets. Although an evaluation of this particular result of electronic surveillance can only be conjectural, there is evidence that it exists and, as FBI documents revealed through the Media, Pa. raid indicate, the creation of such "paranoia" is open intended by law enforcement.

b. The benefits.

Assessing the benefits is at least as difficult as evaluating the costs. There is first the question of the appropriate measure of benefits. An easy measure is counting the number of convictions obtained through electronic surveillance but this would be simplistic but nevertheless difficult.

In the first place, it is necessary to evaluate who is convicted. If, as appears to be the case, the overwhelming number of convictions until now have been of minor offenders, is that a sufficiently valuable result is justify the costs? For example, in 1976, the National Wiretap Commission reported that all but a handful of the gambling taps were on small-time operators, referred to as "mom and pop" bookie operations. NWC Rep. 6; NWC Staff Studies 408. The penalties are usually a fine or a very short jail term. And if some major offenders are caught, how many such convictions are adequate to justify use of electronic surveillance? Suppose the penalties on these are also modest?

In the drug area, effectiveness is also debateable. On the one hand, drug enforcement is the area where electric surveillance is associated with the highest ratio of convictions to installations. Also, the federal government is devoting more and more resources to electronic surveillance for drug enforcement. And even the staff summary of the National Wiretap Commission, while pointing to the shortcomings of this technique for drug enforcement, also noted that:

> Conventional methods, particularly informants are often regarded as being as effective as eavesdropping in solving narcotics cases. This belief is partly based on manpower problems and in part of the fact that narcotics conspriacies are usually more independently structured than gambling organizations and pose greater surveillance difficulties. In some instances the telephone is used infrequently or not at all. If telephones are used, they are frequently public phones, which are difficult to wiretap. Additionally, individuals at the very highest levels are often very surveillance-conscious.
>
> On the other hand importation schemes involving large quantities of narcotics are dependent upon the telephone. As DEA Administrator John Bartels put it, "In many drug trafficking systems, because distances and time factors

> involved, the telephone becomes a necessary part of the drug dealer's trade."
>
> Furthermore, law enforcement officials believe that electronic surveillance is the only investigative method which can uncover ultimate suppliers and the highest-level members of the organization. The possiblity of penetration to this level is the prime reason for court-ordered surveillance in narcotics cases. Financiers simply do not handle the narcotics, and their participation can be disclosed only by overhearing their conversations. According to New York's Special Narcotics Prosecutor, Frank Rogers, no other method is available to tie all the members of a distribution network together. John Bartels of DEA indicated that electronic surveillance was particularly useful where ethnic barriers make physical surveillance and related activities impossible.
>
> NWC Report 146-47

And the NWC described several specific cases providing "evidence of the effectiveness of a well-targeted and executed narcotics surveillance," NWC 147. There apparently are others. Last April, for example, the New York Times reported the successful use of wiretapping to break a $1.65 billion heroin ring. Raab, N.Y. Times, April 11, 1984, p. B1.

Those who see relatively little value to wiretapping point to the fact that high-level figures are rarely caught. As the National Wiretap Commission Staff Study reported, electronic surveillance is said by some to be no more effective than the conventional methods, such as "buy and bust" and "turning" witnesses. NWC 145, 146. Again, according to some, wiretapping has been unable to penetrate the higher levels of the drug trade. In 1982, a state police eavesdropping specialist told Police Magazine (under a promise of anonymity), "The best you usually can hope for is to get the people who actually handle the drugs from day to day." See also NWC 147. The Bronx district attorney's office, which used to wiretap heavily in drug cases, (26 in 1974 alone) has installed just one in the last five years. See Wiretap Reports 1979-83. And overall, the impact on the drug problem seems minimal. Compare New York Times, April, 1984, p. B1 (apparently successful use of electronic surveillance in breaking $1.65 billion heroin ring) with e.g., Wall Street Journal, Nov. 27, 1984, p. 1, "War Against Narcotics By U.S. Government Isn't Slowing Influx. Supplies Remain Abundant Despite More Seizures."

In other serious offenses, such as murder, assault, arson or robbery, or even continuing offenses such as corruption, loan sharking and extortion, the picture is somewhat clearer--electronic eavesdropping does not seem very effective. For example, New York State Special Corruption Prosecutor Maurice Nadjari spent over $1 million on taps and bugs, with virtually no success Brooklyn District Attorney Eugene Gold bugged a trailer for eighteen months and despite claimes of having broken the back of organized crime, came up with no convictions. In New Jersey, on the other hand, now-Judge Herbert Stern eschewed wiretapping, concentrated on account books and convicted numerous corrupt politicians and businessmen.

With respect to organized crime, the primary target for Title III, the results are, at best, mixed with different observers again drawing different conclusions. According to some, electronic surveillance seems unable to penetrate the upper levels of organized crime, except occasionally and accidentally. "You get to a certain level and then you stop" said a Connecticut police intelligence expert. "If you stumble onto something big, it's more by chance than anything else." Others, however, have claimed great success. See Blakey, NWC Report 192-93. The Wiretap Commission summed up its findings as follows:

> When used against conventional conspiracies, electronic surveillance can be highly and uniquely successful. The target is smaller and usually less well insulated than organized crime groups. In such circumstances, when an entire organization is eliminated, as in the Schebergen case, eavesdropping can be very effective.
>
> Where, however, the target is organized in a more complex, hierarchical, and permanent fashion, calculation of success becomes more difficult. Elimination of an entire oraganization as a result of surveillance based on probable cause concering only a few crimes may be impossible. Penetration into the uppermost levels is always difficult and may involve as much luck as perseverance.
>
> Despite the difficulties which may be encountered because of the enduring nature of Organized Crime, the government's efforts with court-ordered surveillance against leading Cosa Nostra figures have resulted in some considerable successes.
> NWC Report 139

And there do appear to be some demonstable successes in using electronic surveillance against organized crime, such as the conviction of Teamsters president Roy Williams. In December 1982, FBI Director William Webster told a congressional committee of great success in fighting organized crime and one commentator noted that "most of these major investigations made extensive use of nonconsensual surveillance," reported in Goldsmith 159 n.951. Also, in commenting on a prior draft of this paper, New York District Attorney Robert Morgenthau reported several major crime investigations involving corruption, usury, fencing and the like, in which indictments were obtained, purportedly through the use of electronic surveillance. In one of these investigations, no prosecutions resulted*, but in a second (the Garment Center Investigation), there were many convictions with some quite heavy sentences; no information as to convictions was provided as of March 15, 1985 with respect to the other investigations mentioned in the Comment, though it may be too early for any convictions on the 1984 investigation. On February 18, 1985, the New York Times reported that a bug installed in the car of a suspected crime leader had produced evidence currently being presented to a grand jury that could lead to the joint indictment of "the five purported crime chiefs in the New York area." N.Y. Times, February 18, 1985, p. B5. See also Butterfield, U.S. Prosecutors Hope to Expose a 'Mafia' at Coming Boston Trial, ibid (tapes of bug on Gennaro Angiulo and family); there have been recent reports of other arrests based on electronic surveillance.

The other major focus of federal tapping is racketeering, where the Carter Administration undertook a major campaign and did a great deal of electronic surveillance: 119 installations in the four years, including an all-time high on room bugs. Racketeering surveillances are also very expensive, but, according to the Administrative Office Report, not overly fruitful. Seventy percent of the 119 have produced nothing so far, and the remaining 30 percent produced about 200 convictions. Although that does not sound bad, the racketeering statute covers so many minor crimes that the overwhelming proportion of these convictions may be for minor matters; without a detailed analysis of the particular cases, it is difficult to evaluate the cost-benefit balance in such cases.

---

*Convictions for criminal contempt for refusing to talk while perhaps useful, do not seem to be what Congress had in mind when it allowed wiretapping for certain substantive offenses.

Insofar as electronic surveillance has not resulted in as many convictions as hoped or anticipated, part of the reason may be that electronic surveillance is not so much a crime detection technique, as an intelligence gathering device. See the Blakey statement quoted at p. 19 above. The latter is probably not a legitimate function under Title III, which is aimed at crime detection, but even if it were, the value and benefits of such intelligence are difficult to assess, for such an assessment requires criteria for evaluating the information obtained, a matter often involving the most subjective kind of judgments.

In assessing these assertions, there is also a causality issue: Was the wiretap or bug indispensable to obtaining the conviction? That is a very difficult question for it requires analysis of a specific cases and a judgment as to both causality and indispensability. A full-scale study of that issue is obviously beyond the scope of this paper. National Wiretap Commission studies, however, cast some doubt on the accuracy of some of the results reported by prosecutors and on claims of causality and indispensability. See, e.g., NWC Staff Studies 331-32; 1955 Hgs. 71,347.

The contrasting views are perhaps best summarized in the contrasting conclusions of the majority and minority of the National Wiretap Commission in 1976:

A. Effectiveness of court-authorized electronic surveillance in criminal investigations.

1. The Commission finds that:

a. General. The considerations which led Congress to provide procedures for court authorization of electronic surveillance for law enforcement are still applicable. The Commission vigously reaffirms the findings and statements of policy made by Congress in 1968 that:

Organized criminals make extensive use of wire and oral communications in their criminal activities. The interception of such communications to obtain evidence of the commission of crimes or to prevent their commission is an indispensable aid to law enforcement and the adminstration of justice.

and that

To safeguard the privacy of innocent persons, the interception of wire or oral communications where none of the parties to the communication has consented to the interception should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court. Interception of wire and oral communications should further be limited to certain major types of offenses and specific categories of crime with the assurances that the interception is justified and that the information obtained thereby will not be misused.

[A substantial minority of the Commission expressed the following views:

When Congress passed Title III of the Omnibus Crime Control and State Streets Act of 1968, it did so in the belief that court authorized electronic surveillance would be "an indispensable aid to law enforcement and the administration of justice." Seven years of experience with the statute, however, have cast serious doubt on the validity of that presumption.

Court authorized wiretapping has been used, in a limited number of instances, to make major cases and has resulted in the conviction of a very small number of upper echelon organized crime figures. More frequently, however, the use of electronic surveillance has proven to be extremely costly, both in dollars and manpower terms, and generally unproductive. Excessive reliance on wiretapping has served to discourage the use of more imaginative and cost-effective law enforcement techniques in many instances. Moreover, even under carefully supervised conditions, court authorized electronic surveillance frequently results in substantial invasions of individual privacy.

Accordingly, it would be appropriate for Congress to reconsider the entire range of issues, theoretical as well as procedural, which underlie Title III.] (brackets in original) NWC 3.

Moreover, the current claims of effectiveness sound very much like the same contentions that were made some eight and twelve years ago, see NWC Report xiii, Blakey Separate Report 195-200, 192 n.30 (1976); Peterson statement, 118 Cong. Rec. S11559 (July 24, 1972). Yet it is now clear that these assessments were over-stated. Thus, in December 1982 Professor Blakey, the author of the Wiretap Act, admitted to a Chicago Tribune reporter, "Up until [the Teamsters surveillance] use of the statute has been wooden, unimaginative and hardly aggressive in the best sense of the word. . . . Authorities tended to focus on petty gambling cases, throws up a wire, leave it in place for twenty days, get five convictions and quit." And he concluded, "Quite frankly, if I thought back in 1968 the was the way the statute would be used, I would not have become involved in drafting it, and had I been a Congressman, I would not have voted for it." Another general perspective comes from former President Richard Nixon, who told John Dean, "[Taps] never helped us. Just gobs and gobs of materials: gossip and bullshitting...the tapping was a very unproductive thing. I've always known that. At least, it's never been useful in any operations I've ever conducted."

c. The court-order protections.

Because electronic surveillance was intended to be a "tool" of last resort," see remarks of Senator John McClellan, 115 Cong. Rec. 23, 240 (1969) (§2518(c) imposes "a requirement designed to make the use of [electronic surveillance] a tool of last resort"); U.S. v. Giordano, 416 U.S. 505, 527, (1974), its use was intended to be limited to a few major crimes, under strict judicial supervision that goes beyond the constitutional minima.

Unfortunately, it appears that judges do not exercise as much control as had been anticipated, especially on the state level. Although the Wiretap Commission found that "the carefully designed Title III controls and procedures have effectively minimized the invasion of privacy in law enforement investigations, but need some modifications to further enhance these protections NWC 11, others disagree," one state prosecutor, for example, told the National Wiretap Commission, "I have not found one judge who take the time to read an ex parte wiretap application." Prosecutors from upstate New York and New Jersey noted that where judges do bother to read the papers, "they will rely in many instances on the identity of the applicant or . . . of the investigator."

Nor is this peculiar to wiretapping. As former Philadelphia District Attorney Arlen Specter told the Wiretap Commission:

> My view is where you have ex parte applications by the prosecuting attorney you are really relying on the prosecuting attorney. I think the statistics gathered and filed by the U.S. Court Administrator bear out the conclusion that virtually all the applications made are approved. I do not think court approval is a realistic safeguard. I think you have to trust the prosecutor and, while I feel that generally prosecutors can be trusted, I do not think the safeguard would be sufficent.
> NWC Hgs. 261-62

This judicial deference to prosecutors may be more common on the state level; testimony before the National Wiretap Commission indicates that federal judges take their responsibilities in these matters far more seriously, often requiring periodic reports, a requirement not imposed by the statute itself.

Moreover, the NWC record is almost ten years old. Although there is no particular reason to think so, it is possible that state procedures have tightened up.

Certain judicial rulings have, however, weakened judical controls on both the state and federal levels. For example, judicial decisions have weakened the "last-resort" "safeguard". See Goldsmith 127. Even the Wiretap Commission noted that the requirement has "often been met by standardized language," NWC xvi, which is simply a polite way of saying that the matter is not treated too seriously.

A particular problem with the judicial supervision system (which also applies to both federal and state levels) results from a combination of inherent technical limitations and judicial decison-making: the absence of any meaningful assurance that the surveillance is being minimized to eavesdrop on as few innocent people and conversations as possible, the heart of a statutory and constitutional protective system. See 18 U.S.C. §2518(5) and Katz v. U.S., supra. In the Scott case discussed above, the Supreme Court ruled that police need not even try to minimize if subsequent judicial review indicates that the surveillance was in fact as minimal as possible. Judges, prosecutors, policemen, and defense lawyers all agree that "minimization" is often difficult and that the statutory mandate is not working. The tap and bug can catch everything, and it takes a very conscientious policeman not to listen, particularly if something that seems titillating to him is being talked about.

It is also difficult to supervise the minimization requirement. Prosecutors and police told the National Wiretap Commission that many police will listen to every conversation, but record only those they think appropriate. Some FBI and narcotics agents in Southern California didn't even do that much; it was accidentally revealed in one case that they had recorded all conversations on "bootleg" cassette tape recorders, while "minimizing" on the tapes to be submitted in court. NWC 182. A New Jersey policeman admitted that even if someone were overhead talking to his lawyer, the police would listen in, and any instruction to "minimize" would be ignored. Id. at 122.

How to limit eavesdropping is often quite difficult even to conceptualize. One federal judge in a major drug case excused the interception of 73 calls between a suspect's babysitter and her friends and classmates with the comment that although these conversations were indeed "teenage trivia . . . the eavesdropper, unless possessed of the prescience of a clairvoyant, could hardly predict when they might be interrupted by an adult with more pressing problems." U.S. v. Bynum, 485 F.2d 490, 502 (2d Cir. 1973). In another drug case, the federal officers argued that "in the investigation on an ongoing narcotics conspiracy such as is involved in this case, it is necessary to intercept and monitor from beginning to end all conversations passing through the tapped telephone because narcotics-related transactions are conducted through code words . . . and conversations that may sound innocuous in the beginning may end up on a narcotics related subject employing such code words." U.S. v. Scott, 331 F.Supp. 233 (D.D.C. 1971).

There are other indications that the "minimization" requirement has little impact. The statute requires prosecutors to report the number of conversations on each interception, and the proportion of those they consider "incriminating." Even by the prosecutors' subjective standards, a very high percentage of the calls intercepted are not incriminating. In 1976, for example, almost 60% of the conversations intercepted on the average tap or bug were so characterized by the prosectutors themselves, even though over 55% of the cases were for gambling, where the percentage of "incriminating" interceptions should be almost 100% since the taps are generally on a phone used almost solely for gambling. In non-gambling contexts, the percentage of crime-related conversations is much lower. For example, in 1970, there were 21 non-drug and non-gambling investigations, in which fewer than 20% of the conversations were allegedly incriminating. In many investigations, none of the conversations overheard were considered incriminating. See H. Schwartz 1973 ACLU study.

Even these averages may be too high, since prosecutors sometimes overstate. In one Queens gambling case, for example, the Wiretap Commission staff found that a five-month long set of three taps had nothing to do with the two minor convictions that were obtained (fines of $500 and $700 were imposed on defendants), but the District Attorney had nevertheless reported that over half of some 1,671 intercepted conversations were incriminating. NWC Staff Studies 331-32. In a federal drug case in California, a judge found that only 5-10% of the conversations yielded useful evidence, though the government prosecutor had reported that 85% were incriminating. U.S. v. King, 335 F. Supp. 542 (D. Calif. 19).

Hard as it is to "minimize" telephone tapping, it is even more difficult to limit a bug, as one New York Supreme Court Justice told the Wiretap Commission, especially if it is placed in areas where there is public access. NWC Hgs. 569. Lawyer-client conversations have frequently been overheard in such situations, and often deliberately. In one Michigan case, federal agents bugged the wrong room, but still continued to listen. In another case, long conversations between housewives about household matters were intercepted in their entirety, the Government's excuse being, "we can't help it. We don't know who is involved."

Another problem for those seeking to enforce the minimization requirement is that the hearing takes a great deal of time and money, and according to some lawyers, judges are not overly sympathetic to such challenges.

Judicial reluctance to enforce vigorously the "other alternatives" and "minimization" requirements is but part of a more general reluctance to enforce legislative and constitutional protections of privacy against law enforcement. Defense lawyers have complained steadily that judges bend over backwards to avoid suppressing illegally obtained evidence. Wiretaps and especially bugs cost so much and take up so much manpower that judges don't want to throw the case away for what they may consider merely "technical" violations, even though the statute seems quite clear in requiring suppression of evidence obtained in ways that don't comply with the statute. See U.S. v. Chavez, 416 U.S. 562 (1974), (exclusion of wiretap evidence appropriate only for important violations even though government officials deliberately deceived the court.)

And if a judge is too sticky, he is simply avoided. The statute throws no obstacles in the way of what lawyers call "judge-shopping," and tough state judges are bypassed. (This is much harder to do in the federal system). One New York prosector explained how easy it was to pick a judge: he simply waits for the court to close for the day, and he can then go to any judge.

It should be noted that these views are not shared by all. Some observers believe the minimization and other requirements are operating very effectively, see Morgenthau Comments. And the National Wiretap Commission majority concluded that "the carefully designed Title III consists and safeguards have effectively minimized the invasion of privacy in law enforcement investigations, but need some modifications to further enhance their protections." NWC 11. Nevertheless, even enthusiastic supporters of Title III believe that the Supreme Court's treatment of the minimization requirement, taken together with certain of its other rulings, have made Title III safeguards against indiscriminate surveillance potentially "meaningless." See, e.g., Goldsmith 111.

d. General implications.

The electronic surveillance experience described above raises serious questions about how effectively our system can cope with any intrusive, wide-ranging technology that is not easily controlled. A combination of judicial laxity--inevitable in any context, as Senator and former Philadelphia District Attorney Arlen Specter had noted--and technical difficulties, creates almost insurmountable control difficulties, even when legislation tries to deal specifically with a particular technique.

These difficulties raise even more serious policy issues in evaluating how to handle these new technologies. Because controls may be so inherently difficult, from both a technical and pratical point of view, the balance of costs and benefits must be struck with especially great care. But in striking such a balance we face a combination of disputable and subjective criteria for need and success, unreliable data as to costs and results, and subjective judgments as to causality and indispensability.

2. Policy options.

Although some tinkering with Title III may be possible, it is doubtful that the major problems discussed above can be dealt with, legislatively or otherwise. Electronic surveillance has become too routine a law enforcement device for it to be politically possible to make any significant changes in the statute to limit its intrusiveness. The efforts this past

Congress to impose some controls on one-party consent surveillance, see H.R. 4826, S. 2669, got nowhere and there is little reason to think that any other measures aimed at increased control would be any more successful. Whatever shortcomings there may be in the original legislation with respect to adequately protecting civil liberties are now probably irreversible.

Nevertheless, if political realities permitted it, there are some very real options, which might protect civil liberties better and also improve the cost-effectiveness of the technique.

1. The most sweeping option would be to abolish all law enforement electronic surveillance, a prospect that is so unrealistic as to warrant no discussion, regardless of the merits of the proposition.

2. An almost equally unrealistic position but one which would probably garner more expert support, is repealing the electronic surveillance authority of state law enforecment officials. Given the power of states rights in the Congress, this proposal is equally unrealistic. Nevertheless, a case can be made for the proposition that because state use is primarily for gambling and relatively minor narcotics enforcement, and because the state courts seem to be performing the worst job of enforcing the statutory safeguards, there is little to lose and much to gain from such a porposal.

A more limited version of this option would entail reducing the crimes for which state officials may use electronic surveillance, by limiting them to serious felonies like murder or kidnapping. This option would, of course, eliminate the authority of New York and Florida to wiretap except rarely and the New York City District Attorney's office, at least, has always used wiretapping to a relatively great extent. That this would seriously interfere with the efforts to prosecute organized crime is dubious, but the political realities are such that this option is also unrealistic.

3. Limiting both federal and state authorities to certain serious crimes, as wiretapping was originally intended to be used, see S. Rep. No. 1097 at 97 ("Each offense has been chosen because it is intrinsically serious or . . . characteristic of the operations of organized crime"), would also seem to make sense: serious narcotics trafficking, defined perhaps in terms of the quantities involved; organized crime offenses, limited perhaps to RICO, usury and corruption; and as a fall-back in an appropriate case, murder, kidnapping and espionage. See Minority Recommendation Id, NWC Report 5. Given the current and approved use of electronic surveillance, this list covers almost all of the relevant offences; one might expand that list, as in H.R. 6343, 98th Cong. 2d Sess. (10/1/84) (Kastenmeier D-Wis.) by including tampering with or retaliating against a witness. See H.R. 6343, §4.

4. Bugging. A minority of the National Wiretap Commission recommended abolishing the authority to install microphone surveillances:

> [B]ugs are far more intrusive on personal privacy than are wiretaps. A hidden microphone picks up every voice within its range, including innocent as well as potentially incriminating conversations, making

> minimization impossible under such circumstances. In addition, bugs planted within a bedroom may give rise to serious invasions of marital privacy. Finally, the installation of a bugging device frequently requires a breaking and entry by law enforement personnel, a procedure of at least questionable propriety, even if authorized by a court.
>
> Weighing these potential privacy infringements against the limited value and use of bugs by law enforecment agents, a minority of the Commission is convinced that the balance on this issue falls on the side of protecting privacy. Accordingly, they would ban the use of bugging devices in non-national security cases.
> NWC 15

However,

> A substantial majority of the Commission, . . . believes that the infrequent law enforcement use of bugs indicates that law enforcement can be trusted to use the method only when absolutely necessary. Further, in a number of successful cases, bugs have provided evidence where wiretaps would have failed. Members of the top levels of conspiratorial crime frequently refuse to conduct their illegal business activities by telephone; if their place of business can be located, a bug can prove useful. The entire scope of conspiratorial plans can be learned; secret meetings can be completely exposed. Ibid.

This option therefore appears equally unrealistic, whatever the merits, which are subject to much dispute.

5. Last resort use. It has been suggested that the statute be amended to require "that the exhaustion statement contain, in effect, an investigative checklist. . .of every alternative reasonably available and an explanation of its inutility." Goldsmith, Statement to House Judiciary Subcommittee of Courts, Civil Liberties and the Administration of Justice, (Jan. 20, 1984) Mimeo 7; see also Goldsmith 129, 131; H.R. 6343 § 6(b). The problem with this approach, however, is that the difficulty is not with what the prosecutors have been presenting, though that has generally been inadequate, Goldsmith, 129 (preprinted

forms "used on occasion"), NWC Report 66, but that the judges have not taken their responsibilities seriously. Thus, although the suggested proposal is a useful step, it is not enough unless there is a clear legislative statement, either in the text of the statute the preamble thereto, or in the legislative history using words like "last resort" and/or "clearly demonstrated" that will send the appropriate message to the judges.

6. Minimization can perhaps be improved if Scott and U.S. v. Kahn, 415 U.S. 143 (1974) (interception of unknown third parties permitted) are legislatively overruled, and Congress insists that there be both a good faith attempt at minimization, and objective minimization given the facts of the particular situation. Unfortunately, sanctions here are especially difficult to enforce. The usual one would be suppression of all the evidence for violation of the good faith requirement, see People v. Brenes, 53 A.D. 2d 79 (1976), aff'd, 42 N.Y. 2d 41 (1977) but few judges are likely to adopt this sanction, though it has been statutorily adopted in New Jersey. N.J. Stat. Ann. § 2A:156A-21 (Supp. 1976), discussed in Carr, Electronic Surveillance, § 5.08, p. 267 (1977) and 1983 Supp; (hereinafter "Carr"). H.R. 6343 provides that such a wholesale suppression may be ordered if the failure to minimize is part of "a pattern of intentional legality," but it is difficult to believe such a pattern will ever be readily demonstrable.

Professor Goldsmith has also suggested that the Kahn decision be partially overruled insofar as it permits surveillance of conversations to which none of the parties are known, by limiting eavesdropping authority "to conversations involving at least one identified party." January 20, 1984 Statement at 9. This proposal, which is also incorporated in H.R. 6343 as § 6(d), amending §2518(4), could minimize the number of innocent persons overheard, and would seem to be in accord with Congress' original intent. See S. Rep. No. 1097 at 101.

A separate suppression remedy might be instituted for eavesdropping on lawyer-client conversation. Such eavesdropping will rarely be justified, and yet it happens not infrequently. Automatic suppression of the entire lawyer-client conversation, might be useful; an even stronger sanction would be to also suppress all interceptions taking place after the privileged conversation.

7. Emergency authority. The statute permits dispensing with a warrant briefly in emergencies involving national security and organized crime. Obviously, there should also be such emergency authority where life is in danger and the statute should be so amended. The problem does not seem acute, but it is a request made by the Justice Department during the Carter Administration and it seems highly reasonable if we are to have any wiretapping at all. Where possible--and it usually will be--telephone authorization should be sought, so that at least a contemporaneous record of the circumstances and some magistrate-approval can be established.

8. Selective suppression for violations. In a ruling seemingly inconsistent with the elaborateness and detail of Title III and a legislative history seemingly pointing to strict

enforcement, the Supreme Court read into the statute an exemption for certain proven violations from the suppression sanction, because they were not "central" to the statutory scheme, U.S. v. Chavez, 416 U.S. 562, 572-74 (1974). As things stand, courts have no guidance except their own values and judgment as to what is "central." See Carr, § 6.03[3][a], pp. 355-57. Congress would do well to try to specify either the specific "central" sections or workable criteria, if there be any, to establish "centrality."

9. Periodic Reports. Many, if not most, federal courts have imposed an extra-statutory requirement that the prosecutors file periodically (e.g., every five days) reports on the interception to assure that it is being done properly and usefully. There is no reason why this same requirement could not be statutorily mandated with respect to both federal and state interceptions.

Adoption of at least the more modest of these proposals would remedy some of the more troubling problems with the statute, such as excessive use and minimization, i.e., the judicial supervision aspects. But at least as important is a clear signal from the Congress that the statute is to be strictly enforced.

It has been suggested that if much of the problem is with judicial application of statutory safeguards (e.g., the minimization and last-resort requirements) such judicial nullification will apply to all legislative efforts, either with respect to improving existing statutes or with legislative treatment of new technologies. But part of the problem is with legislative ambiguity, and if--and it is a large "if"--Congress can give a clear signal, these problems will be at least minimized.

It is doubtful that political support for these measures can be mustered. Despite the view even of scholars sympathetic to law enforcement that judicial rulings and practice have weakened the statutory safeguards, and that changes are necessary, see *e.g.*, Professor Goldsmith, few active law enforcement offices are likely to support these proposals. Given the seriousness of the crime problem, their views are not likely to be disreguarded.

B. National Security Intelligence Surveillance.

The history of national security surveillance follows a pattern similar in many ways to law enforcement surveillance. (1) An early lack of constitutional control--indeed, virtually no Supreme Court cases dealt with this problem before 1972, and many lower court decisions gave the executive branch virtually *carte blanche*, see *U.S. v. Brown*, 484 F.2d 418 (5th Cir. 1973); but see *Zweibon v. Mitchell*, 516 F.2d 594 (D.C. Cir. 1974). (2) There were gross abuses by the executive branch, which were exposed and documented in congressional inquiries though the Government had purported to be operating in accordance with strict administrative procedures, III Church Comm. 292-93, n.71, II Church Hgs. 441-53 (Shattuck testimony); private communication with Ramsey Clark, H. Schwartz *Taps*. (3) There was a major and recent Supreme Court decision imposing some controls on at least *domestic* intelligence gathering, *U.S. v. U.S. District Court (Damon Keith)*, 407 U.S. 297 (1972). And (4), a statute has been passed, the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1800ff.

1. The legislative history of FISA and the statutory framework.

As with law enforcement electronic surveillance Congress concluded that "the law . . . has been uneven and inconclusive . . . threaten[ing] both civil liberties and national security," especially since that law develops "generally in ignorance of the *facts, circumstances* and techniques of foreign intelligence electronic surveillance not before the court". H.R. Rep. No, 95-1283- I, 95th Cong., 2d Sess. 21 (1978). The Congress therefore established a court order system for surveillance of foreign powers and foreign agents. The system generally requires a judicial warrant for most electronic surveillance. Unlike Title III, which is limited to eavesdropping on conversations, FISA applies to all forms of interception including "'beepers' and 'transponders' if a warrant would be required in the ordinary criminal context [where it often is not, see *U.S. v. Knotts,* 460 U.S. 276 (1983). It could also include miniaturized television cameras and other sophisticated data not aimed merely at communications." *Id*. at 52. It does not include physical searches. *Id*. at 53.

The formal legislative history does not tell the whole story. The statute represents elaborate and sustained cooperation among civil liberties groups, Congress and the Justice Department, with much of the focus on whether U.S. persons had to be involved in some kind of criminality before they could be targeted for FISA surveillance. This kind of cooperation, if it could be replicated, would seem one of the best ways to reconcile any tensions between liberty and order.

2. The problems arising out of intelligence surveillance are more acute than with law enforcement. They go far beyond electronic surveillance and apply to any form of intelligence surveillance. They include at least these:

a. The nature of intelligence investigation is to be all-inclusive and necessarily indiscriminate. As is clear from the Blakey testimony described above, where surveillance is directed to a crime, a specific criminal act or event provides at least some criteria for relevance and specificity. But where intelligence surveillance is concerned, there are few guidelines, and the "minimization" requirement becomes almost meaningless. As FBI Director Clarence Kelley said about foreign intelligence investigations:

> In investigating crimes such as bank robbery or extortion, logical avenues of inquiry are established by the elements of the crime. The evidence sought is clearly prescribed by these elements.
>
> But there are no such guidelines in the field of foreign intelligence collection. No single act or event dictates with precision what thrust an investigation should take; nor does it provide a reliable scale by which we can measure the significance of an item of information.
>
> The value and significance of information derived from a foreign intelligence electronic surveillance often is not known until it has been correlated with other items of information, items sometimes seemingly unrelated.
>
> Also, difficulty in determining the potential value of information derivable from such an installation makes it hard

> to predict the required duration of the surveillance. Hearings on Electronic Surveillance for National Security Purposes before the Senate Subcommittees on Criminal Laws and Procedures and Constitutional Rights, 93rd Cong., 2d Sess. 255 (1974).

The same absence of guidelines holds for the gathering of domestic intelligence, as the Supreme Court recognized in the Damon Keith case.

For this reason, surveillance for intelligence purposes lasts much longer than for law enforcement. Compare § 2518(5) of Title III (30 days plus extensions) with 50 U.U.S.C. § 1805(d)(1) (FISA) (90 days or one-year, depending on the target, plus extensions). Since the scope is broader, minimization is conceptually much harder if not impossible, though required by the statute. Thus, it is not surprising that the little evidence we have so far indicates that the number of people and conversations overheard or intelligence surveillances is even greater than with law enforcement surveillance. See H. Schwartz, Taps 38.

b. Oversight and control are also very difficult. For example, the number of FISA surveillances has risen steadily from 319 in 1980 (the first full calendar year that FISA was in effect) to 549 in 1983. An explanation has been offered, see The Foreign Intelligence Surveillance Act of 1978: The First Five Years, S. Rep. No. 98-660, 98th Cong., 2d Sess. (1984), p. 5. The secrecy of the operation--the procedures are in a secret court and FISA does not require notice to the targets--means that little outside scrutiny can take place, however, and there is no way to test this explanation.

It is even more difficult for Congress to determine whether the statute is being used properly. The only way to determine that is to review many individual applications, but as the House Oversight Committee commented in its May 9, 1984 report on wiretapping under FISA, the applications made available to Committee Staff were censored so extensively as "to reduce significantly the utility of the review process." Implementation of the Foreign Intelligence Surveillance Act, H.R. Rep. No. 98-738, 98th Cong., 2d Sess. 4 (1984). The Committee went on to note that Committee members had themselves reviewed a few applications, but concluded:

> Therefore, as noted above, the Committee has based its oversight judgments largely on its review of the Attorney General's semiannual classified reports and on extensive discussion with officials of the Department of Justice, Office of Intelligence Policy and Review, the FBI, and the NSA, in whom the Committee continues to place its trust and confidence.
>
> However, effective oversight must be based on a more permanent foundation than good working relationships. Members of Congress and their staffs, and exectuive [sic] branch officials and their staffs, come and go. Soon, few will remain who were present at the creation of FISA.
>
> With the foregoing in mind, and with the continuing increase in the use of the authority provided by FISA to electronically surveil U.S. persons, and others, the Committee has concluded that its continued ability to state with confidence, as it has in the past, that U.S. person surveillances are being conducted fully within the letter and spirit of the law, must depend on a more thorough review of a larger number unredacted applications by both Members and a limited number of staff selected by the Committee. The Committee expects the Department of Justice to cooperate in this effort.
> Ibid.

The recent report by the Senate Intelligence Committee is a good deal more sanguine about the Act, see S. Rep. No. 98-660 at 23, and notes that "the Committee reviewed selected FISA applications," p.9, but it is not clear whether these were redacted. The secrecy of the process also makes it difficult for voters and even other Senators or experts to determine whether Congress is doing its job, whether the law is being obeyed, and whether changes in the law are necessary.

Even if Congress were able to exercise adequate oversight, it is not clear that it would. Part of the reason for rotating membership on the Senate and House Intelligence Committees is concern that the Committees will be "captured" by the intelligence agencies and not exercise adequate oversight.

The evaluation problem becomes even more acute when deciding on the effectiveness of intelligence surveillance, either in a particular case or in general. What are the criteria for success, when the only results are not even convictions or arrests, but bits and pieces of information, the importance of which may be apparent only to the agency involved? And even then, the significance of much of this information may not be immediately apparent.

Indeed, although Congress assumed that "a real and substantial need for foreign intelligence electronic surveillance--at least under certain defined circumstances-exists," H.R. Rep. No. 95-1283-I, 95th Cong,. 2d Sess. 22 (1978), there is much controversy about the value of electronic surveillance for intelligence purposes even among experts. Former Attorney General Ramsey Clark declared in 1972 that if all national security intelligence taps were turned off, the net adverse impact on national security would be "absolutely zero." Other Attorneys General including Nicholas de B. Katzenbach, Elliot Richardson, and William Ruckelshaus apparently concur, as does former Secretar of State Dean Rusk. See Carr, §53.06 [1], p. 104. Morton Halperin, a former staff member of the National Security Council, has taken the same position. CIA records disclosed that its microphone surveillance of Micronesian official was "wholly unproductive," according to a Senate Intelligence Committee report in April 1977. The Court of Appeals for the Third Circuit found that the taps in one case had been "ineffective and unsuccessful," and the JDL taps did not prevent an Amtorg office bombing. United States v. Ivanov, 324 F. Supp. 928, 937 (D.N.J., 1972), aff'd, 492 F.2d 593, 618-19 (3d Cir. 1974); see Zweibon v. Mitchell, 516 F.2d 594, 609-10 (D.C. Cir. 1975) (en banc). The Church Committee concluded that wiretapping and bugging had been particularly useless with respect to discovering the sources of leaks, despite repeated use of electronic surveillance for this purpose by several Administrations. And many intelligence experts have consistently downgraded the importance of any kind of covert intelligence gathering. Ransom, The Intelligence Establishment, 1-50 (1971), especially Zacharias, id. at 19.

On the other hand, many believe that electronic surveillance is very useful. In view of the secrecy, subjectivity, controversy and inherent uncertainty of these kinds of evaluation, even for members of the intelligence community, can an outside observer make a meaningful evaluation? Can even Congress do so?

c. The problem of oversight and evaluation is compounded by the reluctance of many judges--including those on the secret FISA court--to exercise meaningful review over foreign intelligence matters. For example, the former Chief Judge of that Court, U.S. District Judge George Hart told a House Judiciary subcommittee that the FISA court exercises no supervision after the taps or bugs are installed, in contrast with the practice of many federal judges in Title III surveillances. There is consequently no way of knowing whether federal agents do even the modest minimization required by the Act, even though the FISA statute itself allows the judges "to assess the government's compliance with the minimization procedures applicable to a particular surveillance." 50 U.S.C.A. § 1805(d)(3). Even the relatively sanguine Senate Intelligence Committee seemed a bit concerned that the Court seemed "especially trusting" and "does not make an effort to assess compliance beyond asking occasional questions." S. Rep. No. 98-660, pp. 9, 11, 26.

d. A further problem is that intelligence gathering is inevitably done under looser standards than is law enforcement surveillance, see U.S. v. District Court, supra and this is reflected in differences between FISA and Title III. What if agencies with intelligence-gathering authority, e.g., the FBI, use the looser FISA standards to gather evidence for law enforcement? The courts have not dealt with this too successfully, see S. Rep. No. 98-660 at 12-15; Note, 70 Va.L.Rev.

297, 335-336 (1984). Because it turns on intent, and courts are loath to exclude probative evidence in major cases, a satisfactory resolution of this problem seems unlikely.*

At root, the problem of judical oversight rests on a widespread and understandable attitude among federal judges that "the very nature of foreign intelligence gathering does not lend itself" to traditional Fourth Amendment controls such as minimization, See, e.g., the attitude in U.S. v. Humphrey, 456 F. Supp. 51,56 (E.D. Va. 1978), and U.S. v Brown, supra. Judges are uncomfortable reviewing executive action where foreign affairs are concerned, and at one time, the Supreme Court took the view that anything relating to foreign affairs was immune to judicial scrutiny, Oetjen v. Central Leather Co., 246 U.S. 297, 302 (1918). That position was disapproved in Baker v. Carr, 369 U.S. 186, 211 (1962), but a deferential attitude still prevails. This deference is, of course, not present where domestic intelligence is concerned, see U.S. v. U.S. District Court, supra, but even there, the Court has said it is willing to accept much looser standards for intelligence gathering than for law enforcement. 407 U.S. at 322-24.

All of these problems are aggravated by the historical record of abuses in the name of national security. From the Alien and Sedition Laws to the surveillances by the FBI of Dr. Martin Luther King, Jr. and the many other abusive practices uncovered by the Church Committee, the temptation to use such intrusive devices in an honest or other attempt to protect national security has been a major problem that we have not really solved.

---

* It is not too significant that in some twelve prosecutions where the government offered FISA evidence, the Courts found the applications in order. These cases involve only 12 out of hundreds and, in any event, the Government was not likely to offer poorly prepared papers.

C. One-Party Consent Surveillance.

The issues raised by one-party consent surveillance are very different from those discussed earlier, at least insofar as legal/policy matters are concerned.

The law has always been quite clear. An unbroken series of Supreme Court decisions has ruled in wiretap and other contexts that the secret use of recorders, transmitters or other devices by one party to a conversation is not constitutionally protected. The Court has assimilated the situation to the use of informers without technology, and has reasoned that a person simply assumes the risk that his conversational partner will inform on him, and has, in effect, waived his right to constitutional protection. In U.S. v. White, 401 U.S. 745 (1971), after Katz was decided and a lower court had ruled that a person had "a reasonable expectation of privacy" that his conversation would not be transmitted, the Supreme Court read Hoffa v. U.S., 385 U.S. 293 (1966) to mean that "however, strongly a defendant may trust an apparent colleague, his expectations in this respect are not protected by the Fourth Amendment. . . [and] 'no interest legitimately protected by the Fourth Amendment is involved.'" It went on to rule that the existence of a transmitter made no difference. 401 U.S. at 749,

752. Justices Douglas and Harlan dissented, arguing that a "qualitative difference" existed when electronic transmission of a conversation was involved, quoting Justice Brennan's observations to the same effect in Lopez v. U.S., 373 U.S. 427, 465-66 (1963).

The fundamental difference in attitude over the significance of technology between the dissents and the majority in White (as well as with Justice Jackson's indication in the 1952 On Lee case that "the use of technological devices" to magnify the object of a witness' vision" or hearing, made little constitutional difference) is fundamental. The White decision is clearly supportable in the Court's traditional principles of consent, and it reflects the Court's refusal to move beyond those traditional approaches. This refusal is also reflected in its attitude toward some of the new technologies, to be discussed below.

Because of the Court's approach, there is virtually no constitutional check on one-party consent surveillances, except for some very ambiguous restrictions in Title III on such interceptions by private people, which seem to have had no effect; several state statutes, however, do bar interception unless all parties consent. For a compilation see Carr, §3.05[3].

The Federal establishment prohibits surreptitious taping by a General Services Administration regulation, but this regulation seems to have been regularly ignored. See the Wick incident discussed in House and Senate Hgs. in 1984. The federal law enforcement establishment apparently has internal regulations governing use of transmitters and recorders, but little is known about their operation.

Law enforcement authorities have routinely resisted a warrant requirement for such consent surveillances which, according to some experts, is the most common form of electronic surveillance. See generally Westin, Privacy and Freedom (1967). Their concern is partly that it may be difficult to specify a particular target--the informer may be told simply to infiltrate a group and learn what he can--and partly because the procedure might be cumbersome. The former difficulty often disappears when electronic surveillance is used, for that is usually done when the police zero in on a specific target. As to whether the procedures might be too cumbersome, some prosecutors' offices are already required by local law to obtain prior warrants and, although they resorted to consensual surveillance infrequently, the Wiretap Commission concluded that they "did not feel particularly hindered by this requirement." NWC 118. On the other hand, other prosecutors assert that they will be too burdened by even a modest authorization requirement.

Policy Options

There are several policy options which would not seem to create too cumbersome a set of procedures, and which warrant consideration.

(1) There is no obvious justification for a government official taping a conversation, when that official is in no way connected with law enforcement or intelligence gathering. It may thus be appropriate to amend §2512(c) of Title III to prohibit such taping, where it is not for either law enforcement or

intelligence gathering.

(2) Where law enforcement uses consent surveillance, it may be appropriate to impose administrative controls similar to those requirred under the Privacy Protection Act of 1980, P.L. 96-440, 42 U.S.C. §2000a-11, which allows federal supoenas of non-suspect third parties if done pursuant to Guidelines promulgated by the Attorney General. These Guidelines deal with the problems of privileged communications, among other matters, and could be shaped to prevent such problems as a single person's consent being sufficient to justify a bug of of many people, sometimes including lawyers, etc.

(3) The problem of a single person's consent being sufficient to bug a room full of people, many whom are not targets of an investigation, could be handled by a legislative prohibition on taping or transmitting such multi-party conversations where many, most, or all of the participants are not targets. How serious a problem this is, I don't know but it does seem to come up.

III. New Technologies

A. Judicial Decisions

The Supreme Court and some other courts have grappled with the privacy ramifications of some of the new technologies. Unfortunately, the Court seems to be repeating the precedent it set with Olmstead: an unnecessarily narrow application of traditional concepts in a way that ignores the special problems posed by the increased penetration, miniaturization and cost-reduction of many of these technologies.

A quick glance at the Supreme Court's six decades of grappling with new technologies shows that a Court majority has almost never considered the novel ramifications but has almost invariably chosen a construction that ignores the novelty. Examples that come quickly to mind are Olmstead, of course, as well as Goldman (bug), On Lee and White (transmitters). The Court's prevailing attitude was summed up in Justice Jackson's comment--admittedly pre-Katz--that there is no difference between an intrusion by the naked eye and by a telescope. It is also reflected in Justice White's post-Katz refusal to see any difference between the problems raised when one talks to an informer who is there by himself and when one talks to an informer wired for sound who is transmitting the conversation to hidden third parties.

One problem, of course, with all these devices is their surreptitious quality. An ordinary search is not usually secret, and an inventory of what is seized must be turned over to the target. Supervision and control of the execution of the search, either in advance or after the fact by a suppression hearing, is not difficult. Where the search is surreptitious, such controls are very much harder to impose and enforce.

A review of the new technology cases decided by the Supreme Court shows the Supreme Court's reluctance to grapple with the novel realities. The key cases deal with beepers, pen registers, bank records and drug detection dogs. Lower courts have dealt with videotaping, infra-red and other types of vision-enhancing devices, and helicopter cameras.

The Court has dealt with the beeper twice and come out in different though analytically consistent ways. In *U.S. v. Knotts*, 460 U.S. 276, 103 S.Ct. 1081 (1983), where the beeper enabled the police to monitor *public* movements--*i.e.*, the movement of a chloroform container while the container was in a car travelling on a public highway--no Fourth Amendment protections attached. The Court found no legitimate expectation of privacy in the car's and container's movements on a public highway. The beeper enabled the police to learn what they could have learned had someone stuck with the target throughout the time he was in public--which, of course, nobody had. "Nothing in the Fourth Amendment prohibited the police from augmenting the sensory facilities bestowed upon them at birth with such enhancements as science and technology afforded them in this case," said Justice Rehnquist for the majority, citing the pre-*Katz* decision of *U.S. v. Lee*, 274 U.S. 559 (1927), where the

Court allowed a search of a boat by a searchlight that was not shown to have penetrated "below decks or under hatches." 103 S.Ct. at 1086.

In the second case a year later, U.S. v. Karo, 104 S.Ct. 3296 (1984), the Court ruled that trailing a container into a house and keeping in touch with it there, did violate the Fourth Amendment. The Court found a legitimate expectation of privacy in the house, and an equally legitimate expectation that containers would come into the house without a government surveillance device. The analogy with Hoffa, where a human surveillance device was allowed surreptitiously to enter, was drawn in a partial dissent by Justices O'Connor and Rehnquist, but Justice White dismissed this.

This difference between the home and public areas is one that is likely to be maintained. Lower courts dealing with searchlight and flashlight penetration, as well as the handful dealing with infra-red penetration and with high-powered telescopes, have made this distinction. See cases summarized in I LaFave, Search & Seizure § 2.2, 1984 Supp. p. 74 n.49.1, where use of such devices on people moving in the dark outside their home or in cars was not afforded Fourth Amendment protection, but those inside the house were.

This distinction is somewhat reminiscent of Olmstead's ruling that voices projected outside the house are not protected. Both Knotts and the other cases seem inconsistent with the Katz notion that it is the reasonableness of the expectation of privacy that counts, and no reason is given why it is unreasonable to expect privacy for activities in darkness, whether inside or outside the house.

The problem is obviously with the criterion of "reasonableness" for ascertaining when an expectation of privacy will be respected. What a Justice thinks "society is prepared to recognize as reasonable" is inherently subjective (even though the concept of "reasonableness" purports to be objective--a measure of social valuation), and the Court has provided few criteria. Common sense indicates some distinction between a home and a highway, but drawing distinctions among different intrusions on the home or highway is not easy, for it is indeed true that "society may be prepared to accept as reasonable" even something done or said "in an area accessible to the public." 389 U.S. at 351-52. And though common sense might also have distinguished between the interior of the car and the interior of a home to some extent, it is difficult to grasp intuitively or otherwise the very great differences in constitutional protection the Court has afforded cars and homes, under the "reasonable expectation of privacy" test. See generally LaFave, II Search and Seizure, Ch. 7. (1979).

The Rehnquist language in Knotts minimizing the significance of "scientific enhancement" of the senses is particularly troubling, for all surveillance devices enhance the senses. If Katz is sound, then the question is whether the sense enhancement is so detrimental to privacy, is so intrusive on matters that people want to keep private, that allowing uncontrolled use of it would seriously impair basic values of our society.

The inside-outside distinction is reflected in yet another Supreme Court surveillance decision, one that deals not so much with new technology, but with the consequences of the new information technology and the vast amount of information accumulated in banks, government files, etc.. U.S. v. Miller, 425 U.S. 35 (1976). In Miller, the Court ruled that a person's bank records could be made available to government officials without any Fourth Amendment controls because "all of the documents . . . contain only informations voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business . . . The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the government." This same analysis was used a few years later to allow unrestricted police access to telephone company records. Smith v. Maryland, 442 U.S. 735 (1979). The information was "voluntarily turned over to third parties" -- the telephone company employees.

The limitations of this type of analyis are reminiscent of Olmstead, for it ignores the nature of our industrialized, complex, computerized society, in which we are forced to reveal certain matters to the people who provide us with services like banking, credit, phones, transportation, and the like, but we do not expect that they will reveal it to others. As Professor LaFave has pointed out, "under Smith, the police may without any cause whatsoever and for whatever purpose they choose, uncover private relationships with impunity merely because the telephone company might under some circumstances for certain limited purposes make a record of such relationships for the company's own use." I Search & Seizure, § 2.7, 1983 Supp. 109 (emphasis in original).

A final Supreme Court decision involving not technology but use of an animal for sense "enhancement"--the use of dogs to detect drugs--shows the same unwillingness to explore the ramifications of such sense "augmentation." In U.S. v. Place, 103 S.Ct. 2637 (1983), the Court relied on a totally different matter--the limited nature of the search and a belief that these dogs respond only to the contraband (which turns out not to be the case. See LaFave, I Search & Seizure § 2.2 1984 Supp. 81-82.) But the limited nature of the intrusion--the "canine-sniff . . . does not require opening the luggage . . . [and] expose non contraband items"--is irrelevant to whether something one seeks to keep private is entitled to be respected, at least unless Fourth Amendment protections are complied with. Lower courts have held that magnetometers and X-ray scanners are subject to the Fourth Amendment, and the implications of Place for these is unclear.

The final area--and in some ways, one of the oldest--has not yet reached the Supreme Court: videotaping or the use of cameras. Here, again, the distinction has been drawn between inside and outside. One lower court recently allowed unrestricted use of a zoom camera on a helicopter, and many other cases have ruled similarly. LaFave, I Search and Seizure 528-30 and 1984 Supp.; several courts have allowed a virtually permanent closed-circuit camera to be used in public places. In addition, a New York court has held that standard Fourth Amendment principles apply to videotaping of inside premises, but called for legislation to deal with the special problems posed by the sweeping intrusiveness of such techniques. People v. Teicher, 52 N.Y. 2d 638, 439 N.Y.S. 2d 846 (1981). See 3 Hast. Con. L. Q. 261 (1976). In the very recent case of U.S. v. Torres, __F.2d__, (7th Cir. Dec. 19, 1984), the Court of Appeals held that four of the protections of Title III--a statute which does not apply to video surveillance, though a dissenting Judge argued that it did--would be applied to videotaping because of its very intrusive nature: the last resort requirement, particularity of description, and minimization of the interception in time and scope, see §§ 2518(3)(c), (4)(c) and (5); and were related to the Fourth Amendment requirement of "particularity."

All of the Supreme Court decisions could have gone the other way: there were strong dissents in almost all (except Knotts.) But the Court's record makes it clear that its concern for law enforcement, especially in drug cases (compare Chief Justice Taft's feelings about the Volstead Act, discussed earlier) make it unlikely that a majority will restrain the police in these areas, despite the severe criticism the Court has received for these discussions even by experts like Professor LaFave, who has not usually been unsympathetic to law enforcement needs. (Compare the reaction to Olmstead, discussed above.)

The sweep of the one-party consent doctrine--that constitutional protection to a transaction evaporates when one party to that transaction consents to the surveillance--is especially in need of reconsideration in light of the new sweeping technologies like videotaping and the greater availability and efficiency of bugging devices. If carried to its logic, the one-party consent waiver doctrine would allow a minor or casual participant in a multi-person transaction or a visitor to consent to the installation of cameras or microphones on everyone else so long as he is a participant to some degree. For example, in the _Hoffa_ Case, the informer Edward Partin, an old friend of Hoffa's, was simply a bystander to most of what occurred in Hoffa's hotel suite during Hoffa's trial. Should Partin have been allowed to give the police permission to videotape or bug everyone else in that suite?

Even in the two-party transactions involved in _White_ and _On Lee_, why is society "_not_ prepared the recognize as reasonable" the expectation that a person you are talking to is not _transmitting_ the conversation to a third person? Perhaps it is not "reasonable" to assume that there is no recording going on, either by memory or machine, but surely letting a third person listen in, is different. The Court's answer seems to be some notion of "assumption of risk" by "one contemplating illegal activities". 401 U.S. at 752-53. But what of innocent people whose conversations are being transmitted? Surely, Justice Harlan's analysis of the "assumption of risk" fiction is more realistic. Before noting that the majority result also subjects "each and every law-abiding member of society to the risk," he explained the special harm from electronic transmission as follows:

> The argument of the plurality opinion, to the effect that it is irrelevant whether secrets are revealed by the mere tattle-tale or the transistor, ignores the differences occasioned by third-party monitoring and recording which insures full and accurate disclosure of all that is said, free of the possibility of error and oversight that inheres in human reporting.
>
> Authority is hardly required to support the proposition that words would be measured a good deal more carefully and communication inhibited if one suspected his conversations were being transmitted and transcribed. Were third-party bugging a prevalent practice, it might well smother that spontaneity--reflected in frivolous, impetuous, sacrilegious, and defiant discourse--that liberates daily life. Much off-hand exchange is easily forgotten and one may count on the obsurity of his remarks, protected by the very fact of a limited audience, and the likelihood that the listener will either overlook or forget what is said, as well as the listener's inability to reformulate a conversation without having to contend with a documented record. All these values are sacrificed by a rule of law that permits official monitoring of private discourse limited only by the need to locate a willing assistant. Id. at 787-89 (footnotes omitted).

Unfortunately, these bursts of judicial realism occur almost exlusively in dissents.

Two other doctrines that need reconsideration are the inside-outside distinction and the implications the Court insists on drawing from a person's exposure to third party service-providers who have the most minimal and limited interest in the contents. As Justice Stewart recognized in Katz, much of what we do outside, may be entitled to privacy. Surely if a person walks in a park and talks in whispers with a companion, that conversation is entitled to be protected from a parabolic microphone 100 yards away. Similarly, why should someone who meets another person in the dark in order to keep their identities confidential, not be entitled to the privacy of the dark, and especially to be free from prolonged observation by cameras that can photograph in the dark without any indication of their presence?

There is an even greater need for some kind of protection with these new technologies, than with older techniques like flashlights, etc. Many of these new devices facilitate surreptitiousness by being invisible and thus not calling attention to themselves and alerting the target. This, of course, is nothing new--the use of binoculars or cameras is equally invisible. But the combination of much greater penetration and secrecy means that much more long-term, undeterrable surveillance is possible, lulling people into a false sense of security and facilitating the disclosure of confidences, whether pertinent or not, to the investigation.

To put it differently, the difference in degree between the capacity for continuous long-term surveillance of the new and old technologies is so great, as to be a difference in kind with respect to the impact on privacy. It is this factor that the Supreme Court has ignored. The problem will be made more acute as technology advances. A paper by Robert Corn, Esq., of Washington, D.C., points out that cellular telephone technology, whereby people in transit can communicate by telephone wherever they are by a portable wireless phone, will open up new possibilities for continuous or spot surveillance. Through computer tracking at the Mobile Telephone Switching Office, which locates each mobile unit geographically even if it is not currently in use, it will probably be possible to know where a person is at all times. If the Court's current "beeper" analysis stays in effect, there will be no constitutional protection against that kind of tracking, for almost by definition, the mobile phone user is "outside"

Indeed, the logic of this "inside-outside" "public exposure" conceptual framework is so far-reaching, that it has the logical capacity to undermine current protections. Most telephone communications, not just cellular, are transmitted by radio wave, which go out over the air. The new Olmstead-type thinking could assimilate this to exposing one's conversations to outside witnesses, thus robbing it of protection. It is unlikely that the logic will indeed be extended so far, but the potential for a law enforcement oriented court is there.

As to the other aspects of the problem--the "voluntary exposure to third parties"--such exposure is an inevitable feature of modern life, and it is impossible to avoid such disclosures. As one commentator put it:

> Dramatic increases in urbanization and technology have caused property and privacy interests to diverge. Economic specialization has largely supplanted the individual's house or papers as repositories for personal information; computers are more efficient. There is today dependence upon hospitals and doctors' offices rather than upon bedside physicans, telephonic communications rather than direct conversation, and bank-intermediated transactions in place of direct payments, all of which generate second or third party records. Rather than suppress personal information or confine it to his home, which would be--if not impossible--grossly inefficient and severely restrictive of social and financial intercourse, the individual chooses third party intermediaries whom he believes will protect his privacy. Custom, statutory restrictions, and private remedies serve to enforce these expectations of privacy. Yet, under a "proprietary interests" interpretation of the Fourth Amendment, these nonproperty modes of informational control go unrecognized: Privacy is protected only if embodied in a proprietary relationship.

Note, 83 Yale L.J. 1439, 1458-59 (1974), quoted in LaFave, p. 412.

Administrative self-restraint cannot be depended upon either. A recent House of Representatives report on the use of informers and traps makes that clear once again. See Executive Summary of Report on FBI Undercover Operations, Comm. Print No.12, Subcommittee on Civil and Constitutional Rights of House Judiciary Committees, 98th Cong., 2d See. 23-25 (1984). (Operation Corkscrew). It is thus necessary for legislation to resolve these issues, for carefully tailored approaches that will balance the needs of law enforcement and other governmental missions with the maintenance of values basic to our society. Although neither the courts nor Congress have shown themselves to be consistently solicitous of privacy interests, legislation imposing some controls would be better than the virtually uncontrolled situation we have today with respect to many of these devices and practices.

Policy Options

Several policy options will be set out here. Because these problems are, for the most part, relatively new, and in some cases at least may require novel approaches, the proposals are suggested for consideration and analysis, rather than for action.

1. Title III. One option, of course, is simply to include pen registers, videotaping and beepers under Title III, as H.R. 6343 seems to do. The same could be done with FISA, by amending

it so as not to exclude devices--like beepers and pen registers--currently excluded from protection by the Fourth Amendment.

2. Beepers. It may be thought that the Title III procedures are too elaborate for the lesser intrusion involved when the beeper is only on outdoor activities. The issue raised by the outdoor beeper is very difficult and profound: how much protection is to be provided to the search for anonymity and privacy in a crowd? It is clear that where First Amendment values are involved, some courts have insisted on limitations on certain police activities, such as photographing demonstrations and public meetings. So far, almost no courts have formally granted legal protection for such public activities that may implicate First Amendment interests. Where, as in the normal law enforcement situation, no such First Amendment concerns are threatened, the case for full protection is even weaker.

It may therefore by appropriate to develop a lesser degree of protection, calling for some judicial authorization for beeper surveillance of external activities, including perhaps a lesser standard of reasonable belief as a predicate, such as reasonable suspicion. There would seems to be no need to dispense with a warrant, since haste in the installation of a beeper is rarely likely to be necessary, and some degree of neutral antecedent scrutiny would seem to be a virtually indispensable protection.

3. Pen Registers. Again, the full Title III procedures may be unnecessary because of the more limited nature of the intrusion from a pen register. But unlike a beeper, which simply registers outdoor location, a pen register can provide

information that a person is very eager to keep private--whom he or she is calling. One can certainly argue--and all nine Justices agreed on this--that one who goes outside is indeed waiving privacy to some extent; that "waiver" is in no way implicit in a telephone call, and it is very difficult to understand why there should be so much less protection for the identity of a party called, than for the contents of the call itself. The notion that a telephone call is a "voluntary exposure" of the telephone number is simply unrealistic and unwarranted--one cannot avoid such an "exposure" if one makes a call, and most people would probably assume it is as free from police intrusion as the call itself. There is no reason for Congress to accept the Court's approach.

For this reason, there is a much better case for including pen registers under Title III and FISA. If, however, that is considered too great an interference with law enforement, there is certainly no reason why a conventional warrant requirement should not be imposed, in accordance with the standard usages of Rule 41(b) of the Federal Rules of Criminal Procedure.

4. Videotaping. H.R. 6343 recognizes the enormously intrusive nature of videotaping by not only bringing it under Title III, but by imposing additional prerequisites to its use: a 10-day limitation on orders and extensions (as opposed to 30 days for wiretap and bugs), and resort to electronic audio surveillance before audio surveillance is authorized. See H.R. 6343, §8.

One problem with H.R. 6343 is that the bill is not clear with respect to how video surveillance with the consent of one party is treated: it seems to be treated like audio surveillance (with the two exceptions note above.) If so, it has serious defects of the kind discussed above, in the discussion of video surveillance.

I am informed that in the hearings conducted by Congressman Kastenmeier preceding introduction of H.R. 6343, there was little dicussion of videotaping. Hearings focused on that issue alone would seem useful.

It should be noted, finally, that the Torres decision discussed above imposes certain minimal constitutional requirements based on the Fourth Amendment's particularity conditions. Legislation is therefore necessary to go beyond these rather minimal matters.

IV. Illegal Electronic Surveillance
By Private Parties and Foreign Goverments.

A. Private Parties.

It was hoped that enactment of Title III would make it possible to prosecute and thereby reduce private electronic surveillance often used in domestic matters and industrial espionage. Indeed, this was one of the purposes of the legislation. See S. Rep. No. 1097, 90th Cong., 2d Sess. 67 (1968). The practice was made illegal under Title III (as it had been under the predecessor §605), and subject to heavy penal and civil penalties.

There is no reason to believe this hope has been realized. Indeed, because the device is so surrepititous and hard to detect, there is little hard data on which to make any judgments, except for the number of prosecutions, which, necessarily is the merest tip of the iceberg, though it would be useful to ascertain the number of successful prosecutions for violations of Title III since 1968. All we have is anecdotal evidence as specific incidents of illegal activity come to light, and some inconclusive studies by the National Wiretap Commission.

As to the latter, in 1976 the full Wiretap Commission agreed that "the enforcement of Title III by prosecution of illegal eavesdroppers has been disappointing." NWC 23. While asserting that the amount of illegal eavesdropping has declined (a conclusion supported by no hard data because neither the Commission nor anyone else know how much illegal wiretapping goes on) the Commission noted the indifference of many law enforcement officials, including the FBI, to illegal private or official eavesdropping.

The most common area for illegal private tapping may be in marital disputes, though there seems to be a substantial amount in business and industrial matters as well. Judges seem quite uninterested in imposing sanctions against wiretapping in family matters. NWC 24.

The Watergate break-in is just one of many examples of lawless wiretapping by people in or associated with government. Since 1968, there have been many revelations of illegal police wiretapping: In New York City, for example, there was a major bribery scandal involving 40 members of a Special Investigations Unit of the New York City Police Department which dealt with narcotics violations. In Houston, the police were suspected of illegal wiretapping by a new police chief, and the FBI refused to look into the matter; according to the chief, "either they [the FBI] were totally aware of what was going on and approved of it, or they were totally incompetent." Hearings on Wiretapping before the Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the House Judiciary Committee, 94th Cong., 1st Sess., at 406 (1975) (Houston, Texas, Chief of Police Carrol Lynn). Chicago police and Pennsylvania State Police have also been involved in illegal surveillance. New Haven police illegally tapped the phones of over 100 people from 1966 to 1971, with the knowledge of the Mayor. NYT, Jan. 25, 1977, p.37. In a case involving clearly illegal taps by the Mayor of Williamsport, Pa., local FBI agents who knew of them again chose not to investigate. II NWC Hgs. 1348. The Law Enforcement Assistance Administration has apparently subsidized purchases of wiretap equipment by police agencies in states which had not given the police wiretap authority.

Despite all this, the Justice Department unit authorized to prosecute these violations consists of only a few lawyers who have many other responsibilities. During 1969-74, only 75 people were convicted of violating Title III and another 46 cases ended in dismissal or acquittal.

The secrecy of electronic surveillance devices, and the difficulties of determining who placed them, and whether anything was actually overheard, make it next to impossible to know how widespread the practice, to prosecute detected cases, and to evaluate whether the law has had any effect in reducing the incidence.

B. Foreign Government Surveillance

The above difficulties are compounded when the surveillance is by foreign goverments, for the crudities and lack of sophistication in technological technique which can facilitate detection of illegal private eavesdropping, are not likely when the surveillance is by foreign governments. The practice is, of course, equally illegal.

To cope with this problem, President Reagan has issued National Security Directive 145 to try to protect American govermental communications against such surveillance by scrambling telephone conversations to prevent eavesdropping. According to the New York Times of Oct. 15, 1984 (p. A20), the Directive states that eavesdropping equipment "is being used extensively by foreign nations," and can also be "employed by terrorist groups and criminal elements." Although not specifying whether any such eavesdropping had in fact occurred--an omission probably dictated by security reasons--the order apparently relied on intelligence reports that such eavesdropping is a serious security threat.

The New York Times further reported that the directive established a cabinet-level steering committee to formulated overall policy, to oversee systems security resources programs, and to coordinate and executive technical activities.

The directive does raise civil liberties concerns. For example, the order explicitly authorizes the agency to monitor "official communications in strict compliance with the law, Executive Orders and applicable Presidential directives." Though the directive does not authorize the monitoring of the communications of private corporations, guidelines under which such monitoring may be conducted were approved by Attorney General William French Smith earlier this year in a letter to Lincoln D. Faurer, director of the security agency. Those guidelines allow the Government to "monitor telecommunications systems which are owned or leased by Government contractors for their own use" if the government obtains the "express written approval of the chief executive officer of the contractor organization," and provides "adequate notice to the contractor organization's employees."*

The problems in dealing with such foreign surveillance are manifold. For one thing, how can it be detected? Although it is quite likely that the intelligence agencies are aware of a good deal of it, the actual dimensions of such surreptitious conduct can only be guessed at. For example, a recent article in a popular magazine consists almost exclusively of speculation ("If the Soviet Union were targeting Boeing telephones, it might well have picked up the memo;" five "intercept posts" were described, but no facts were stated as to whether they in fact did any interception. Kahn, The Bugging of America, Penthouse Oct. 1984, pp. 69ff.

---

*The background and ramifications of this directive can be further explored if useful.

Secondly, will measures taken in respond to such surveillance impinge on the rights of Americans? How? Can this be guarded against? Minimized?

Third, how can the Executive Branch's activities in this area be monitored by Congress? Should they be? Even if they should, will they be? What criteria are to be applied in evaluating such measures? Who should do it--a special congressional committee like the Intelligence Committee? The Foreign Relations Committee? The Judiciary Committee?

In few areas, are the civil liberties issues more complex and troubling than in national security, and particularly with respect to such counterintelligence matters as are involved in a response to foreign government surveillance. Yet, 200 years of American history, and particularly the events of the 1960s-1970s, make it clear that such counterintelligence measures pose a severe threat to the very values such measures are designed to protect.

History of Electronic Surveillance
Key Events

1924	Attorney General Harlan F. Stone prohibits Electronic Surveillance by Bureau of Investigation.
1928	**Olmstead v. U.S.**, 277 U.S. 438 excludes telephone tapping from constitutional protection.
1931	Attorney General William Mitchell retracts Stone ban on electronic surveillance
1933	Congress prohibits electronic surveillance for Prohibition law enforcement.
1934	Congress enacts Communications Act, including §605.
1938	U.S. Supreme Court construes §605 as barring wiretapping by federal officials. **Nardone v. U.S.**, 302 U.S. 379 (1938).
1938	Each House of Congress passes a bill to overturn Nardone, but differences between the bills are not reconciled and no legislation passes.
1939-40	Department of Justice construes §605 as barring only the combination of interception and divulgence, thereby enabling the Government to intercept so long as it does not use evidence in court or "divulge" outside the Department.
1940	President Franklin D. Roosevelt authorizes limited electronic surveillance for national security purposes.
1942	U.S. Supreme Court applies Olmstead to rule that microphone surveillance not involving a physical intrusion into protected premises does not implicate the Fourth Amendment; Court also holds that such surveillance is not within scope of §605. **Goldman v. U.S.**, 316 U.S. 129 (1942).
1946	President Harry S. Truman extends 1940 authorization for national security surveillance to domestic criminality involving organized crime.
1949-55	Revelations of widespread governmental surveillance by federal and state officials.
1954	U.S. Supreme Court implicitly overrules one aspect of Olmstead by ruling that intangible conversations are protected by the Fourth Amendment. **Irvine v. California**, 347 U.S. 128 (1954).
1954	Attorney General Herbert Brownell authorizes

	"unrestricted" FBI microphone surveillances "in the national interest" without Attorney General approval, even when a trespass is involved.
1957	U.S. Supreme Court rules that §605 prohibits wiretapping by state officials **Benanti v. U.S.**, 355 U.S. 96 (1957).
1957	Apalachin, N.Y. meeting of suspected organized crime figures.
1959	Publication of Dash, Schwartz & Knowlton, *The Eavesdroppers*, documenting widespread wiretapping.
1963	Revelation of illegal FBI and IRS electronic surveillance.
1965	President Lyndon B. Johnson prohibits all electronic surveillance except for national security purposes.
1967	U.S. Supreme Court overrules trespass requirement of *Olmstead* and indicates constitutional requirements for a valid electronic surveillance statute. **Katz v. U.S.**, 389 U.S. 347 (1967), and **Berger v. New York**, 388 U.S. 41 (1967).
1968	Title III of Omnibus Crime Control & Safe Streets Act enacted, authorizing electronic surveillance by federal and local officials for law enforcement purposes.
1971	U.S. Supreme Court reaffirms that electronic surveillance with consent of one party to conversation is not within Fourth Amendment protection. **U.S. v. White**, 401 U.S. 745 (1971).
1972	U.S. Supreme Court rules that intelligence gathering about domestic matters must be in accordance with Fourth Amendment protections, including judicial authorization. **U.S. v. U.S. Dist. Ct.**, 407 U.S. 297 (1972).
1976	U.S. Senate Select Committee to Study Government Operations With Respect to Intelligence Activities issues report finding serious abuses of constitutional rights by intelligence agencies.
1976	National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance issues report and publishes studies on experience under Title III.
1978	Foreign Intelligence Surveillance Act of 1978 enacted, authorizing court-approved electronic surveillance for intelligence-gathering purposes of conversations and other activities by foreign powers or foreign agents.

LEGISLATIVE HISTORY OF BILLS INTRODUCED IN THE CONGRESS DURING PERIOD 1914–59, WHICH WOULD PROHIBIT WIRETAPPING AND EAVESDROPPING OR AUTHORIZE WIRETAPPING AND EAVESDROPPING BY FEDERAL AGENTS UNDER CERTAIN CIRCUMSTANCES

THE LIBRARY OF CONGRESS,
LEGISLATIVE REFERENCE SERVICE,
October 2, 1959.

To: Hon. THOMAS C. HENNINGS, Jr.,
Chairman, Senate Constitutional Rights Subcommittee
(Attention: Mr. Slayman):

The attached information is forwarded in response to the inquiry from your office noted below:

Respectfully,

HUGH L. ELSBREE,
Director, Legislative Reference Service.

The attached report, "Legislative History of Bills Introduced in the Congress During Period 1914–59, Which Would Prohibit Wiretapping and Eavesdropping or Authorize Wiretapping and Eavesdropping by Federal Agents Under Certain Circumstances," and exhibits pertaining thereto, are in response to your request of December 12, 1958.

PROPOSED LEGISLATION

63d Congress

None.

64th Congress

None.

65th Congress

S. 4954. Mr. Bankhead; September 23, 1918 (Post Office and Post Roads):

Providing for the protection of the users of the telephone and telegraph service and the properties and funds belonging thereto during governmental operation and control. (No action.)

Copy of section prohibiting wiretapping, exhibit 4.

H.R. 12898. Mr. Moon; September 7, 1918 (Post Office and Post Roads):

Providing for the protection of the users of the telephone and telegraph service and the properties and funds belonging thereto during Government operation and control. (No action.)

Copy of section prohibiting wiretapping, exhibit 1.

H.R. 12976. Mr. Moon; September 20, 1918 (Post Office and Post Roads):

Providing for the protection of the users of the telephone and telegraph service and the properties and funds belonging thereto during governmental operation and control (Public No. 230, 65th Cong., 40 Stat. 1017).

Reported in House (H. Rept. 800), September 21, 1918.

Passed by House, September 25, 1918.

Referred to Senate Committee on Interstate Commerce, September 26, 1918.

Reference changed to Committee on Post Office and Post Roads, October 10, 1918.

Source: Hearings before the Senate Subcommittee on Constitutional Rights, Committee on the Judiciary, Part 4, 86th Cong., 1st Sess. (1959).

Reported in Senate, October 14, 1918.
Passed Senate, October 24, 1918.
Approved, October 29, 1918.
Copy of Public Law 230, 65th Congress, exhibit 2.

NOTE.—The report of the House Committee on the Post Office and Post Roads (H. Rept. 800) did not indicate that public hearings on this bill were held.

Copy of House Report 800, 65th Congress, exhibit 3.

66th Congress

None.

67th Congress

None.

68th Congress

None.

69th Congress

H.R. 9071. Mr. White of Maine; March 3, 1926 (Merchant Marine and Fisheries):

For the regulation of radio communications, and for other purposes (Public Law 632, 69th Cong., 44 Stat. 1162).
Reported in House (H. Rept. 404) (see also H. Rept. 404), March 5, 1926
Passed House, March 15, 1926.
Referred to Senate Committee on Interstate Commerce, March 16, 1926.
Reported in Senate (S. Rept. 772), May 8, 1926.
Passed Senate, amended, July 2, 1926.
Conference report (H. Rept. 1886):
Agreed to in House, January 29, 1927.
Agreed to in Senate (S. Doc. 200), February 18, 1927.
Approved February 23, 1927.
Copy of section of bill pertaining to interception of messages, exhibit 5.
Copy of statute pertaining to interception of messages, exhibit 6.

NOTE.—Public hearings were held in connection with H.R. 5589; H.R. 9108; and S. 1754, 69th Congress, which were prior bills similar to H.R. 9071, enacted as Public Law 632. In reporting H.R. 9071 both the House and Senate committees stated that the section dealing with unauthorized reception of messages was a redraft of existing law. (See act of August 13, 1912; 37 Stat. 302.) No indication could be found that public hearings pertaining to eavesdropping or interception of messages were held.

70th Congress

None.

71st Congress

S. 6061. Mr. Hawes; January 26, 1931 (Judiciary):
To prohibit wiretapping in the District of Columbia. (No action.)
Copy of bill, exhibit 10.

H.R. 4139. Mr. Clancy; June 19, 1929 (Judiciary):
To prevent wiretapping. (No action.)
Copy of bill, exhibit 7.

H.R. 5416. Mr. Schafer of Wisconsin; November 21, 1929 (Judiciary):
To prohibit the tapping of telephone and telegraph lines and prohibiting the use of information obtained by such illegal tapping to be used as evidence in the courts of the United States in civil suits and criminal prosecutions. (No action.)
Copy of bill, exhibit 8.

Comments: On February 4, 1931, Senator Hawes proposed an amendment to the bill (S. 3344) supplementing the National Prohibition Act for the District of Columbia. This amendment would prohibit the inter-'eption of telegraphic and telephonic communications in the District of 'olumbia.

(S. 3344 was not enacted.)

Copy of amendment intended to be proposed, exhibit 9.

72d Congress

S. 1396. Mr. Blaine; December 10, 1931 (Judiciary):
To render evidence obtained by wiretapping inadmissible in the Federal courts. (No action.)
Copy of bill, exhibit 12.

H.R. 23. Mr. Clancy; December 8, 1931 (Judiciary):
To prevent wiretapping. (No action.)
Copy of bill, exhibit 11.

H.R. 5305. Mr. Boileau; December 10, 1931 (Judiciary):
To render evidence obtained by wiretapping inadmissible in Federal courts. (No action.)
Identical to S. 1396, see exhibit 12.

H.R. 9893. Mr. Schafer; February 27, 1932 (Judiciary):
To prohibit the tapping of telephone and telegraph lines and prohibiting the use of information obtained by such illegal tapping to be used as evidence in the courts of the United States in civil suits and criminal prosecutions, and for other purposes. (No action.)
Copy of bill, exhibit 13.

Comments: The act making appropriations for the Departments of State and Justice and for the Judiciary for the Departments of Commerce and Labor, for the fiscal year ending June 30, 1934, was amended on the floor of the House to prohibit use of any of such funds for or in connection with wiretapping. This amendment was enacted into law as a part of Public, No. 387, 72d Congress (47 Stat. 1381).

73d Congress

S. 2910. Mr. Dill; February 27, 1934 (Interstate Commerce):
To provide for the regulation of interstate and foreign communications by wire or radio. (No action.)

NOTE.—Section 605 of this bill was similar to section 605f of S. 3285, as introduced. See exhibit 14.

S. 3285. Mr. Dill; March 28, 1934 (Interstate Commerce):
To provide for the regulation of interstate and foreign communications by wire or radio.
Reported in Senate (S. Rept. 781), April 19, 1934.
Passed by Senate, May 15, 1934.
Referred to House Committee on Interstate and Foreign Commerce, May 21, 1934.
Reported in House (H. Rept. 1850), June 1, 1934.
Passed by House, June 2, 1934.
Conference report (H. Rept. 1918):
Agreed to in Senate, June 9, 1934.
Agreed to in House, June 9, 1934.
Approved June 13, 1934, Public, No. 416, 73d Congress (48 Stat. 1064).
Copy of section 605 of bill as introduced, exhibit 14.
Copy of section 605 of enactment, exhibit 15.

NOTE.—Section 605 was amended by the House Committee on Interstate and Foreign Commerce. Committee analysis of section 605 (both identical), exhibit 16.

H.R. 8301. Mr. Rayburn; February 27, 1934 (Interstate and Foreign Commerce):
To provide for the regulation of interstate and foreign communications by wire or radio. (No action.)

NOTE.—Section 505 of this bill is similar to section 605 of S. 3285 as introduced. See exhibit 14.

74th Congress

None.

75th Congress

S. 3756. Mr. Wheeler; January 5, 1938 (Interstate Commerce):
To prohibit the use of communications facilities for criminal purposes.
Reported in Senate (S. Rept. 1790), May 12, 1938.
Passed by Senate, May 18, 1938.
Referred to House Committee on Interstate and Foreign Commerce, May 20, 1938.
Reported in House (H. Rept. 2656), June 8, 1938.

Passed by House, amended, June 15, 1938.
(Failed of enactment.)
Copy of bill as introduced, exhibit 17.
Copy of bill as reported in House, exhibit 18.

NOTE.—This bill passed the House as amended by the House committee. The Senate failed to act on the amended bill.

H.R. 9908. Mr. Lea; March 10, 1938 (Interstate and Foreign Commerce):

To prohibit the use of communication facilities for criminal purposes. (No action.)

NOTE.—Substantially identical to S. 3756 as introduced. See exhibit 17.

76th Congress

House Joint Resolution 553. Mr. Celler; May 27, 1940 (Judiciary):

To authorize the Federal Bureau of Investigation of the Department of Justice to conduct investigations in the interest of national defense, and for that purpose to permit wiretapping. (No action.)

Copy of bill, exhibit 19.

House Joint Resolution 571. Mr. Celler; August 7, 1940 (Judiciary):

To authorize the Federal Bureau of Investigation of the Department of Justice to conduct investigations in the interest of national defense, and for that purpose to permit wiretapping in certain cases.

Reported in House (H. Rept. 2574), June 14, 1940.
Passed by House, August 6, 1940.
Referred to Senate Committee on Interstate Commerce, August 7, 1940.
Copy of bill as passed by House, exhibit 20.

77th Congress

H.R. 2266. Mr. Hobbs; January 16, 1941 (Judiciary):

To amend the Judicial Code by adding thereto a new section authorizing for the purpose of detecting or preventing crime any investigational agency of the United States, when specifically authorized by the head of the department of which it is a part, to intercept, listen in on, or record telephone, telegraph, radio, or any other similar messages or communications; and making such authorizations and communications, and testimony concerning same, admissible evidence; and for other purposes. (No action.)

Copy of bill, exhibit 21.

H.R. 3099. Mr. Walter; February 5, 1941 (Judiciary):

To amend the Judicial Code by adding thereto a new section 274e, relating to the interception of wire or radio communications by persons employed in the investigation, detection, or prevention of offenses against the United States. (No action.)

Copy of bill, exhibit 22.

H.R. 4228. Mr. Hobbs; March 31, 1941 (Judiciary):

To amend the Judicial Code by adding thereto a new section authorizing, for the purpose of detecting or preventing certain crimes, the Federal Bureau of Investigation of the Department of Justice, when specifically authorized by the Attorney General of the United States, to intercept, listen in on, or record telephone, telegraph, or radio messages or communications, and making such authorizations and communications, and testimony concerning same, admissible evidence; and for other purposes.

Reported in House (H. Rept. 358), April 1, 1941.
Failed of passage in House, June 30, 1941.
Copy of bill as reported in House, exhibit 23.

H.R. 6919. Mr. Hobbs; April 13, 1942 (Judiciary):

To amend the Judicial Code by adding thereto new sections authorizing authorized agents of the Military Intelligence Division of the War Department, or of the Office of Naval Intelligence of Navy Department, or of the Federal Bureau of Investigation of the Department of Justice, to intercept, listen in on, or record telephone, telegraph, cable, radio, or any other similar messages or communications, and making such authorizations and communications and testimony concerning same admissible evidence; requiring telegraph and cable companies to furnish such agencies with copies of communications in their possession or under their control upon request; providing punishment for violations, and for other purposes. (No action.)

Copy of bill, exhibit 25.

House Joint Resolution 273. Mr. Celler; January 27, 1942 (Judiciary):

To authorize the Federal Bureau of Investigation of the Department of Justice, and the Intelligence Services of the State, War, and Navy Departments, to conduct investigations in the interest of national defense, and for that purpose to permit wiretapping in certain cases. (No action.)

Copy of bill, exhibit 24.

House Joint Resolution 283. Mr. Celler; February 12, 1942 (Judiciary):

To authorize the Federal Bureau of Investigation of the Department of Justice, the Military Intelligence Division of the War Department, and the Office of Naval Intelligence of the Navy Department to conduct certain investigations in the interest of prosecution of the war. (No action.)

Similar to House Joint Resolution 304. See exhibit 26.

House Joint Resolution 304. Mr. Celler; April 21, 1942 (Judiciary):

To authorize the Federal Bureau of Investigation of the Department of Justice, the Military Intelligence Division of the War Department, and the Office of Naval Intelligence of the Navy Department to conduct certain investigations in the interest of prosecution of the war.

Reported in House (H. Rept. 2048), April 23, 1942.
Recommitted to Committee on the Judiciary, May 4, 1942.
Copy of bill as recommitted to committee, exhibit 26.

House Joint Resolution 310. Mr. Celler; May 5, 1942 (Judiciary):

To authorize the Federal Bureau of Investigation of the Department of Justice, the Military Intelligence Division of the War Department, and the Office of Naval Intelligence of the Navy Department in the conduct of certain investigations in the interests of prosecution of the war, to make use of intercepted communications without regard to the limitations contained in section 605 of the Communications Act of 1934 (48 Stat. 1103), and for other purposes.

Reported in House (H. Rept. 2079), May 7, 1942.
Passed by House, May 26, 1942.
Referred to Senate Committee on Interstate Commerce, May 27, 1942.
Copy of bill as referred to Senate committee, exhibit 27.

78th Congress

House Joint Resolution 41. Mr. Celler; January 7, 1943 (Judiciary):

To authorize the Federal Bureau of Investigation of the Department of Justice, the Military Intelligence Division of the War Department, and the Office of Naval Intelligence of the Navy Department in the conduct of certain investigations in the interest of prosecution of the war, to make use of intercepted communications without regard to the limitations contained in section 605 of the Communications Act of 1934 (48 Stat. 1103), and for other purposes. (No action.)

Substantially identical to House Joint Resolution 310, 77th Congress. See exhibit 27.

79th Congress

None.

80th Congress

S. 2833. Mr. Wiley; January 18, 1948 (Judiciary):

To amend section 605 of the Communications Act of 1934 in order to increase the security of the United States, and for other purposes. (No action.)

Copy of bill, exhibit 28.

81st Congress

S. 595. Mr. McCarran; March 15, 1949 (Judiciary):

Relating to the internal security of the United States.

Reported in Senate (S. Rept. 427), May 27, 1949. Indefinitely postponed, December 15, 1950, 16593.

Copy of section 5 of bill as introduced, dealing with interception, etc., of communications, exhibit 29.

NOTE.—The committee reported a bill in the nature of a substitute. The reported bill did not contain any provisions dealing with the interception of communications. The provisions of the committee bill were passed in another form.

H.R. 3563. Mr. Walter; March 15, 1949 (Judiciary):

Authorizing acquisition and interception of communications in interests of national security. (No action.)

Copy of bill, exhibit 30.

H.R. 3044. Mr. Clemente; March 21, 1949 (Interstate and Foreign Commerce):

To amend section 605 of the Communications Act of 1934 to prohibit the interception of communications, and for other purposes. (No action.)

Copy of bill, exhibit 31.

H.R. 4048. Mr. Clemente; April 6, 1949 (Interstate and Foreign Commerce):

To amend section 605 of the Communications Act of 1934 to prohibit the interception of communications and the possession of intercepting devices, and for other purposes. (No action.)

Copy of bill, exhibit 32.

H.R. 4124. Mr. Kennedy; April 8, 1949 (Interstate and Foreign Commerce):

To make wiretapping unlawful without regard to whether any information so obtained is divulged, to make unlawful the possession of wiretapping equipment with intent to use such equipment for the unlawful interception of wire communications, to authorize the Federal Government to obtain certain information for the national security and defense, and for other purposes. (No action.)

Copy of bill, exhibit 33.

H.R. 9929. Mr. Keating; December 18, 1950 (Judiciary):

To authorize acquisition and interception of communications in interests of national security and defense. (No action.)

Copy of bill, exhibit 34.

82d Congress

H.R. 406. Mr. Walter; January 3, 1951 (Judiciary):

Authorizing acquisition and interception of communications in interests of national security. (No action.)

Substantially identical to H.R. 3563, 81st Congress. See exhibit 30.

H.R. 479. Mr. Keating; January 3, 1951 (Judiciary):

To authorize acquisition and interception of communications in interests of national security and defense. (No action.)

Substantially identical to H.R. 9929, 81st Congress. See exhibit 34.

H.R. 1947. Mr. Celler; January 23, 1951 (Judiciary):

To regulate the interception of communications in the interests of national security and the safety of human life. (No action.)

Copy of bill, exhibit 35.

83d Congress

S. 832. Mr. Wiley; February 6, 1953 (Judiciary):

To authorize acquisition and interception of communications in interest of national security and defense. (No action.)

Identical to H.R. 9929, 81st Congress. See exhibit 34.

S. 2753. Mr. Potter; January 18, 1954 (Judiciary):

To allow admission of certain types of evidence in the Federal courts of the United States against defendants prosecuted for treason, espionage, and other crimes involving the national security. (No action.)

Copy of bill, exhibit 38.

S. 3229. Mr. McCarran; March 31, 1954 (Judiciary):

To prohibit wiretapping by any persons other than a duly authorized law enforcement officer engaged in the investigation of offenses involving the internal security of the United States. (No action.)

Copy of bill, exhibit 39.

H.R. 408. Mr. Celler; January 3, 1953 (Judiciary):

To regulate the interception of communications in the interest of national security and the safety of human life. (No action.)

Identical to H.R. 1947, 82d Congress. See exhibit 35.

H.R. 477. Mr. Keating; January 3, 1953 (Judiciary):

To authorize acquisition and interception of communications in interest of national security and defense. (No action.)

Identical to H.R. 9929, 81st Congress. See exhibit 34.

H.R. 3552. Mr. Walter; February 20, 1953 (Judiciary.)

Authorizing acquisition and interception of communications in interest of national security. (No action.)

Identical to H.R. 3563, 81st Congress. See exhibit 30.

H.R. 5149. Mr. Reed of Illinois; May 12, 1953 (Judiciary):

To authorize the use in criminal proceedings in any court established by act of Congress of information intercepted in national security investigations. (No action.)

Copy of bill, exhibit 36.

H.R. 7107. Mr. Clardy; January 11, 1954 (Judiciary):

To permit the use of certain evidence intercepted by Federal law enforcement officers in the course of investigations in connection with the national security. (No action.)

Copy of bill, exhibit 37.

H.R. 8649. Mr. Keating; March 31, 1954 (Judiciary):

To authorize the admission into evidence in certain criminal proceedings of information intercepted in national security investigations, and for other purposes.

Reported in House (H. Rept. 1461), April 1, 1954.

Passed by House, April 8, 1954.

Referred to Senate Committee on the Judiciary, April 14, 1954.

Copy of bill as reported, exhibit 40.

Copy of bill as passed by House, exhibit 41.

H.R. 8709. Mr. Smith of Mississippi; April 12, 1954 (Interstate and Foreign Commerce):

To amend the Communications Act of 1934 to prohibit the interception of communications by persons other than public officers and employees in the exercise of their official duties. (No action.)

Copy of bill, exhibit 42.

H.R. 9011. Mr. Celler; May 5, 1954 (Judiciary):

To amend title 18, United States Code, with respect to intercepted communications. (No action.)

Copy of bill, exhibit 43.

84th Congress

H.R. 76. Mr. Celler; January 5, 1955 (Judiciary):

To amend title 18, United States Code, with respect to intercepted communications. (No action.)

Identical to H.R. 9011, 83d Congress. See exhibit 43.

H.R. 762. Mr. Forrester; January 5, 1955 (Judiciary):

To authorize the admission into evidence in certain criminal proceedings of information intercepted in national security investigations, and for other purposes. (No action.)

Substantially identical to H.R. 8649, 83d Congress, as passed by House. See exhibit 41.

H.R. 867. Mr. Willis; January 5, 1955 (Judiciary):

To authorize the admission into evidence in certain criminal proceedings of information intercepted in national security investigations, and for other purposes. (No action.)

Substantially identical to H.R. 8649, 83d Congress, as passed by House. See exhibit 41.

H.R. 4276. Mr. Smith of Mississippi; February 22, 1955 (Interstate and Foreign Commerce):

To amend the Communications Act of 1934 to prohibit the interception of communications by persons other than public officers and employees in the exercise of their official duties. (No action.)

Identical to H.R. 8709, 83d Congress. See exhibit 42.

H.R. 4513. Mr. Celler; March 1, 1955 (Judiciary):

To prohibit wiretapping except by a court-authorized Federal officer engaged in the investigation of crimes against the security of the United States. (No action.)

Copy of bill, exhibit 44.

H.R. 4728. Mr. Curtis of Massachusetts; March 8, 1955 (Judiciary):

Making unauthorized wiretapping a criminal offense. (No action.)

Copy of bill, exhibit 45.

H.R. 5096. Mr. Keating; March 21, 1955 (Judiciary):

To authorize the admission into evidence in certain criminal proceedings of information intercepted in national security investigations, and for other purposes.

Similar to H.R. 8649, 83d Congress, as passed by House. See exhibit 41.

NOTE.—This bill contains provisions which would prohibit wiretapping unless authorized by sender or recipient or authorized Federal or State agent in accordance therewith.

85th Congress

S. 2418. Mr. Cotton; June 27, 1957 (Judiciary):

To authorize certain investigative officers of the United States, with the approval of the Attorney General, to intercept and disclose under stated conditions wire and radio communications in the detection and prosecution of offenses against the security of the United States, and for other purposes. (No action.)

Identical to H.R. 377, 86th Congress, exhibit 51.

S. 3013. Messrs. McClellan, Ives, Erwin, Mundt, Goldwater, and Curtis; January 16, 1958 (Interstate and Foreign Commerce):

To amend section 605 of the Communications Act of 1934 to authorize certain communications to be intercepted in compliance with State law, and for other purposes. (No action.)

Copy of bill, exhibit 46.

H.R. 104. Mr. Celler; January 3, 1957 (Judiciary):

To prohibit wiretapping except by a court-authorized Federal officer engaged in the investigation of crimes against the security of the United States. (No action.)

Identical to H.R. 70, 86th Congress, exhibit 50.

H.R. 269. Mr. Keating; January 3, 1957 (Judiciary):

To authorize the admission into evidence in certain criminal proceedings of information intercepted in national security investigations, and for other purposes. (No action.)

Identical to H.R. 5096, 84th Congress. See exhibit 41 and H.R. 5096 note.

H.R. 1010. Mr. Willis; January 3, 1957 (Judiciary):

To authorize the admission into evidence in certain criminal proceedings of information intercepted in national security investigations, and for other purposes. (No action.)

Substantially the same as H.R. 8649, 83d Congress, as passed by House. See exhibit 41.

H.R. 8340. Mr. Hiestand; June 24, 1957 (Judiciary):

To authorize certain investigative officers of the United States, with the approval of the Attorney General, to intercept and disclose under stated conditions wire and radio communications in the detection and prosecution of offenses against the security of the United States, and for other purposes. (No action.)

Identical to S. 2418, 85th Congress. See exhibit 51.

H.R. 9352. Mr. Walter; August 19, 1957 (Un-American Activities):

To amend the Internal Security Act of 1950, and for other purposes. (No action.)

This bill contains a section which would add section 1016 to chapter 93 of title 18, United States Code. This section is substantially the same as S. 2418, 85th Congress. See exhibit 51.

H.R. 9937. Mr. Walter; January 13, 1958 (Un-American Activities):

To amend the Internal Security Act of 1950, and for other purposes. (No action.)

This bill contains a section which would add section 1916 to title 18, United States Code. This section is substantially the same as S. 2418, 85th Congress. See exhibit 51.

H.R. 10232. Mr. Forrester; January 23, 1958 (Judiciary):

To authorize the admission into evidence in certain criminal proceedings of information intercepted in national security investigations, and for other purposes. (No action.)

Substantially the same as H.R. 5096, 84th Congress. See exhibit 41 and H.R. 5096 note.

H.R. 12393. Mr. Keating; May 8, 1958 (Judiciary):

To authorize the interception of communications by certain investigative agencies of the Government, to establish a procedure for the admission into evidence of information so obtained, and for other purposes.

Copy of bill, exhibit 47.

H.R. 12394. Mr. Keating; May 8, 1958 (Judiciary):

To amend chapter 223 of title 18 of the United States Code to permit the introduction into evidence of certain communications intercepted by State law enforcement officers, and for other purposes. (No action.)

Copy of bill, exhibit 48.

H.R. 13842. Mr. Keating; August 21, 1958 (Judiciary):

To prohibit eavesdropping under certain circumstances, and for other purposes. (No action.)

Copy of bill, exhibit 49.

86th Congress, 1st session

H.R. 70. Mr. Celler; January 7, 1959 (Judiciary):

To prohibit wiretapping except by a court-authorized Federal officer engaged in the investigation of crimes against the security of the United States. (No action.)

Copy attached, exhibit 50.

Identical to H.R. 104, 85th Congress.

H.R. 377. Mr. Hiestand; January 7, 1959 (Judiciary):

To authorize certain investigative officers of the United States, with the approval of the Attorney General, to intercept and disclose under stated conditions wire and radio communications in the detection and prosecutions of offenses against the security of the United States, and for other purposes. (No action.)

Copy attached, exhibit 51.

Identical to S. 2418, 85th Congress.

H.R. 2232. Mr. Walter; January 12, 1959 (Un-American Activities):

To amend the Internal Security Act of 1950, and for other purposes. (No action.)

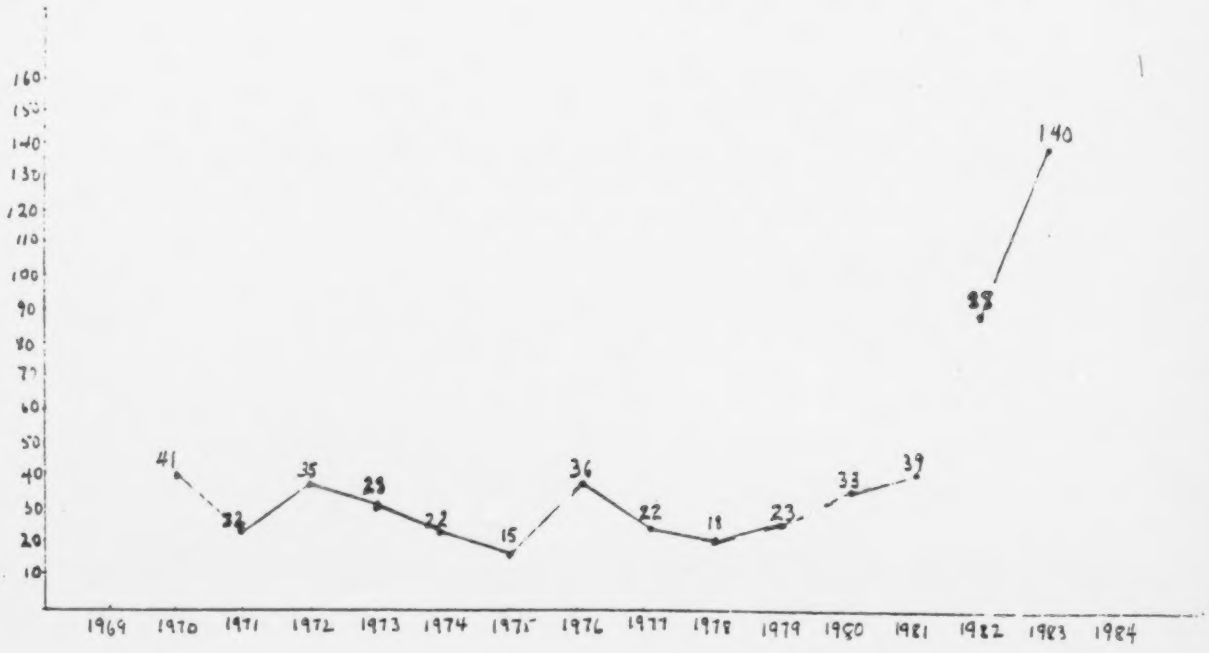
Identical to H.R. 9937, 85th Congress. See exhibit 51 and H.R. 9937 note.

S. 1292. Mr. Keating; March 5, 1959 (Judiciary):

To prohibit eavesdropping under certain circumstances and for other purposes. (No action.)

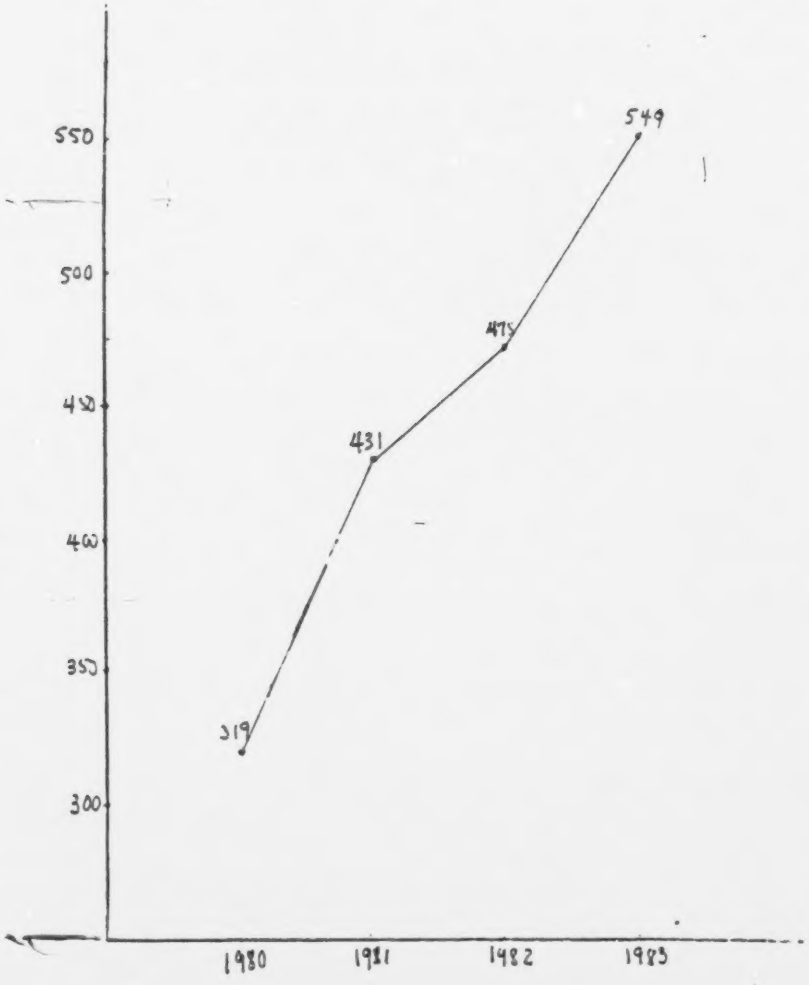
Copy of bill, exhibit 52.

Federage Electronic Surveillances In Narcotics Cases 1970-83



Source: Annual Reports On Applications for Orders Authorizing Or Approving The Interception of Wire or Oral Communications, Administrative Office of the U.S. Courts, 1970-83.

Foreign Security Intelligence Surveillance
Applications Approved 1980-83



Source: The Foreign Intelligence Surveillance Act of 1978: The First Five Years, S. Rep. No. 98-660, 98th Cong., 2d Sess. 2 (1984).

BIBLIOGRAPHY

Books and Articles

M. Abram, Foreward to H. Schwartz *Taps, Bugs and Fooling The People* (1977)

Carr, *Electronic Surveillance* §5.08 (1977) and 1983 Supp.

Dash, R.F. Schwartz and Knowlton, *The Eavesdroppers* (1959)

Goldsmith, *The Supreme Court and Title III: Rewriting The Law Of Electronic Surveillance* 74 J. Crim. L. & Criminology 1 (1983)

Harris, R., *Annals of Legislation--The Turning Point*, The New Yorker 69-179 (Dec. 14, 1968)

LaFave, *Search and Seizure* (3 volumes) (1979) With Annual Pocket Parts

Lowenthal, *The Federal Bureau of Investigation* (1950)

Murphy, *Wiretapping on Trial* (1965)

Navasky, *Kennedy Justice* (1971)

New York Times, February 18, 1985, Butterfield, *U.S. Prosecuters Hope to Expose a 'Mafia' at Coming Boston Trial*

New York Times, Jan. 25, 1977, p. 37.

New York Times, Oct. 15, 1984 p. A20.

Note, 83 Yale L.J. 1439 (1974)

Raab, N.Y. Times, April 11, 1984, p. B1.

Ransom, *The Intelligence Establishment* (1971)

H. Schwartz, *How Do We Know FISA Is Working*? The Nation, Oct 29. 1983.

H. Schwartz, *Taps, Bugs, and Fooling The People* (1977).

Wall Street Journal, Nov. 27, 1984, p. 1. "War Against Narcotics By U.S. Government Isn't Slowing Influx. Supplies Remain Abundant Despite More Seizures."

Westin, *Privacy and Freedom* (1967)

Westin, *The Wire-Tapping Problem*, 52 Colum. L. Rev. 164 (1952) 53 Harv. L. Rev.

3 Hast. Con. L. Q. 261 (1976) 53 Harv. L. Rev. 870 (1940)

70 Va. L. Rev. 297 (1984)

Reports

Congressional Committee Reports and Bills on Electronic Surveillance, 1914-59, reprinted Hearings Before the Subcommittee on Constitutional Rights of The Senate Judiciary Committee, Part 4, Appendix to part 3, 86 Cong., 1st Sess. (1959)

S. Rep. No. 1097, 90th Cong., 2d Sess. (1968)

Reports of Applications for Orders Authorizing or Approving the Interception of Wire or Oral Communications (Wiretap Report), issued by the Administrative Office of the U.S. Courts. 1968-83.

Report of the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance together with Staff Studies and Hearings (1976).

Warrentless FBI Electronic Surveillance, Supplementary Detailed Staff Reports, Book III, Final Report of the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities, 94th Cong., 2d Sess. (1976)

H.R. Rep. No. 95-1283-I, 95th Cong., 2d Sess. (1978) (Foreign Intelligence Surveillance Act of 1978).

The Foreign Intelligence Surveillance Act of 1978: The First Five Years, S. Rep. No. 98-660, 98th. Cong., 2d Sess. (1984)

Executive Summary on Report on FBI Undercover Operations, Comm. Print No. 12, Subcommittee on Civil and Constitutional Rights of House Judiciary Committees, 98th Cong., 2d Sess. (1984)

Congressional Hearings

Wiretapping Hearings Before Subcomm. No. 5 House of Representatives Judiciary Committee, 84 Cong., 1st Sess. (1955)

Invasions of Privacy, Hearings Before the Subcommittee on Administrative Practice and Procedure of the Senate Judiciary Committee, 89th Cong. (1965-66)

Hearings on Controlling Crime Through More Effective Law Enforcement Before the Subcommittee on Criminal Laws and Procedures of the Senate Judiciary Committee, 90th Cong., 2d Sess. (1967)

Hearings on Wiretapping Before the Subcommittee on Courts, Civil Liberties, and the Administrative of Justice of the House Judiciary Committee, 94th Cong., 1st Sess., (1975)